1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-334227**
(43)Date of publication of application : **22.11.2002**

(51)Int.Cl. G06F 17/60
G06F 15/00
H04L 9/08
H04L 9/32

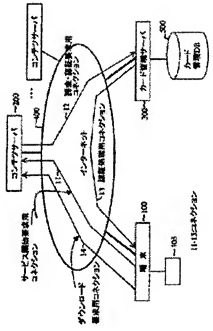
(21)Application number : **2001-140168**
(22)Date of filing : **10.05.2001**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**
(72)Inventor : **SUWA YUICHI**

(54) **PAY SERVICE PROVISION METHOD, PAY SERVICE PROVISION SYSTEM, CONTENT SERVER, PROGRAM FOR PAY SERVICE PROVISION, AND RECORDING MEDIUM**

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a pay service provision method which is available even for a person not owning a credit card and can surely provide pay contents.
SOLUTION: In the pay service provision system, a terminal, a content server providing the terminal with the contents and a prepaid information management server performing the charging processing of pay services are connected to a network. The content server receives the completion report of authentication and charging from the prepaid information management server, then provides the terminal with the pay contents, generates a permission ID validating the downloading of the pay contents within a fixed limited range and transmits it to the terminal. Further, in the case that the downloading of the pay contents is requested again by using the permission ID from the terminal, the contents of the pay service are provided for the terminal within the fixed limit.

図 2



CLAIMS

[Claim(s)]

[Claim 1]A terminal and a content server which provides contents to said terminal, A prepaid information management server which performs accounting of pay service is a pay service provision method in a pay service provision system connected to a network, and said terminal, Using prepaid information media holding predetermined information required for dealings, require use of said pay service from said content server, and said content server, Attestation of whether to have the qualification for said prepaid information media using pay service of said contents to said prepaid information management server, Require fee collection to said prepaid information media, and said prepaid information management server, After performing accounting to said prepaid information media with attestation of said prepaid information media, Perform a completion notification of attestation and fee collection to said content server, and said content server, After receiving a completion notification of attestation from said prepaid information management server, and fee collection, while providing contents of said pay service to said terminal, Generate permission ID which validates download of contents of said pay service in the range within a fixed limit, transmit to said terminal and further. A pay service provision method characterized by providing contents of said pay service in said fixed limit to said terminal when a download request of contents of said pay service occurs again using said permission ID from said terminal.

[Claim 2]The pay service provision method according to claim 1, wherein said content server provides contents of said enciphered pay service to said terminal and said terminal decrypts contents of said enciphered pay service.

[Claim 3]A pay service provision method in a pay service provision system by which a terminal and a content server which provides contents to said terminal characterized by comprising the following, and a prepaid information management server which performs accounting of pay service are connected to a network.

Using prepaid information media holding predetermined information required for dealings, require said terminal from said content server, and use of said pay service said content server, Attestation of whether to have the qualification for said prepaid information media using pay service of said contents to said prepaid information management server.

Prepaid use ID which requires fee collection to said prepaid information media and by which said prepaid information management server was stored in said prepaid

information media to said terminal.
Require transmission with a password of said prepaid information media, andsaid terminal, While transmitting said prepaid use ID to said prepaid information management server, Attest with a predetermined authentication method using said password, transmit to said prepaid information management server, and a password of said prepaid information media said prepaid information management server, Said prepaid information media are attested using said password attested with said predetermined authentication method, And search a database based on said prepaid use ID, and said charge request amount of money from the balance and said content server of prepaid information media of said prepaid use ID is referred to, Said both prepaid information management servers are the balances of prepaid information media to said terminal, when accounting is performed to said balance of said prepaid information media when said balance of said prepaid information media is larger than said charge request amount of money, and said attestation and said accounting are successful.

[Claim 4]A terminal and a content server which provides contents to said terminal, A prepaid information management server which performs accounting of pay service is a pay service provision method in a pay service provision system connected to a network, and said terminal, Require a service menu from said content server using prepaid information media holding predetermined information required for dealings, and said content server, Transmit to said terminal and a service menu said terminal, When service which a user uses is chosen, require use of pay service from said content server, and said content server, Attestation of whether to have the qualification for said prepaid information media using pay service of said contents to said prepaid information management server, Require fee collection to said prepaid information media, and said prepaid information management server, While operation information for attestation is transmitted to said terminal while requiring transmission of prepaid use ID stored in said prepaid information media from said terminal, and said terminal transmits said use ID to said prepaid information management server, A predetermined operation is performed to a password of said prepaid information media using said operation information for attestation, Transmit to said prepaid information management server, and the result of an operation concerned said prepaid information management server, As opposed to said password of said prepaid information media stored in a database, While performing the same operation as an operation which said terminal used using said operation information for attestation,

comparing with the result of an operation concerned and the result of an operation transmitted from said terminal and attesting said prepaid information media, Search a database based on said prepaid use ID, and said charge request amount of money from the balance and said content server of prepaid information media of the prepaid use ID concerned is referred to, When said balance of said prepaid information media is larger than said charge request amount of money, perform accounting which reduces said balance of said prepaid information media, and said prepaid information management server, When both said attestation and said accounting are successful, while notifying completion information of pay service use procedure, and information containing the balance of prepaid information media to said terminal, A completion notification of attestation and fee collection, and said operation information for attestation or said result of an operation is transmitted to said content server, While said content server enciphers contents of pay service and provides said terminal with them, using said operation information for attestation, or said result of an operation as a common key, Generate permission ID which validates download of contents of said pay service in the range within a fixed limit, and it transmits to said terminal, Said terminal is received, when download of contents of said pay service results unsuccessful in said terminal and a download request of contents of said pay service occurs again using said permission ID from said terminal, A pay service provision method, wherein it provides contents of said pay service in said fixed limit and said terminal decrypts contents of said enciphered pay service, using said operation information for attestation, or said result of an operation as a common key.

[Claim 5]The pay service provision method according to claim 3 or 4, wherein a password of said prepaid information media is entered into said terminal from the exterior.

[Claim 6]A terminal and a content server which provides contents to said terminal, A prepaid information management server which performs accounting of pay service is the pay service provision system connected to a network, and said terminal, Prepaid information media holding predetermined information required for dealings are used, A means to require use of pay service from said content server, A means to receive contents of said pay service from said content server, A means to receive permission ID which validates download of contents of said pay service in the range within a fixed limit from said content server, Have a means to require download of contents of said pay service again from said content server, using said permission ID, and said content server, Attestation of whether to have the qualification for said prepaid information media using pay service of said contents to said prepaid information

management server, A means to require fee collection to said prepaid information media, and a means to provide contents of said pay service to said terminal based on a completion notification of attestation from said prepaid information management server, and fee collection, A means to generate said permission ID and to transmit to said terminal based on a completion notification of attestation from said prepaid information management server, and fee collection, When a download request of contents of said pay service occurs again from said terminal using said permission ID, Have a means to provide contents of said pay service in said fixed limit to said terminal, and said prepaid information management server, A pay service provision system provided with attestation of said prepaid information media, a means to perform accounting to said balance of said prepaid information media, and a means to perform a completion notification of attestation and fee collection to said content server.

[Claim 7]The pay service provision method according to claim 6, wherein said content server is provided with a means to encipher contents of said pay service provided for said terminal and said terminal is provided with a means to decrypt contents of said enciphered pay service.

[Claim 8]A pay service provision system comprising:

A terminal.

A content server which provides contents to said terminal.

A means to require a service menu from said content server using prepaid information media which a prepaid information management server which performs accounting of pay service is the pay service provision system connected to a network, and hold predetermined information which needs said terminal for dealings.

A means to require use of pay service from said content server if service which a user uses is chosen, A means to transmit prepaid use ID stored in said prepaid information media to said prepaid information management server, A means to receive operation information for attestation transmitted from said prepaid information management server, to perform a predetermined operation to said password using said operation information for attestation, and to transmit the result of an operation to said prepaid information management server, A means to receive permission ID which validates download of contents of pay service in the range within a fixed limit from said content server, From said content server, have a means to receive contents of said pay service, and said content server, A means to transmit a means to transmit a service menu to said terminal, and address information of said terminal and accounting information of said pay service to said prepaid information management server, A means to require

attestation of whether to have the qualification for said prepaid information media using pay service of said contents, and fee collection to said prepaid information media of said prepaid information management server, and attestation from said prepaid information management server, And a means to provide contents of said pay service to said terminal based on a completion notification of fee collection, A means to generate said permission ID and to transmit to said terminal based on a completion notification of attestation from said prepaid information management server, and fee collection, Said terminal is received when a download request of contents of said pay service occurs again using said permission ID from said terminal, Have a means to provide contents of said pay service in said fixed limit, and said prepaid information management server, A means to transmit said operation information for attestation to said terminal, and a means which attests said prepaid information media with a predetermined authentication procedure using a password of said prepaid information media, A means to search a database based on said prepaid use ID, and to perform accounting to the balance of prepaid information media of the prepaid use ID concerned, and a means to transmit a completion notification of attestation and fee collection to said content server.

[Claim 9]Said prepaid information management server is provided with a means to transmit information for attestation used as an encryption key, to said content server, and said content server, Have a means to encipher contents of pay service by using as a common key information for attestation transmitted from said prepaid information management server, and said terminal, The pay service provision system according to claim 8 having further a means to decrypt contents of said enciphered pay service, by using said certification information as a common key.

[Claim 10]Operation information for attestation to which said information for attestation is transmitted from said prepaid information management server to said terminal, Or the pay service provision system according to claim 9 being the result of an operation which performed a predetermined operation in said terminal to a value which combined said operation information for attestation, and a password.

[Claim 11]It is a content server which provides contents of pay service to a terminal, As opposed to a prepaid information management server connected via a network from said terminal according to a demand using prepaid information media holding predetermined information required for dealings of pay service use, Attestation of whether to have the qualification for said prepaid information media using pay service of said contents, A means to require fee collection to said prepaid information media,

and a means to provide contents of said pay service to said terminal based on a completion notification of attestation from said prepaid information management server, and fee collection, A means to generate permission ID which validates download of contents of said pay service in the range within a fixed limit based on a completion notification of attestation from said prepaid information management server, and fee collection, and to transmit to said terminal, A content server having a means to provide contents of said pay service in said fixed limit, to said terminal when a download request of contents of said pay service occurs again using said permission ID from said terminal.
[Claim 12]KO according to claim 11 characterized by **, comprising:
[Claim 12]. . It is a service menu to said terminal.
****** -- a means, and address information of said terminal and accounting information of said pay service -- said prepaid information management server.
A means to **, and information for attestation transmitted from said prepaid information management server are used as a common key, and they are contents of pay service.

[Claim 13]A terminal and a content server which provides contents to said terminal, . A prepaid information management server which performs accounting of pay service can set to a pay service provision system connected to a network. A procedure of making a service menu requiring of said content server using prepaid information media which are the programs for pay service offer which control said terminal, and hold predetermined information required for dealings, A procedure of making use of pay service requiring from said content server when service which a user wants to use is chosen, A procedure to which said prepaid information management server is made to transmit prepaid use ID stored in said prepaid information media based on a demand from said prepaid information management server, A procedure of performing a predetermined operation to a password of said prepaid information media, and making the result of an operation transmitting to said prepaid information management server using operation information for attestation transmitted from said prepaid information management server, Aprocedure of making permission ID which validates download of contents of said pay service in the range within a fixed limit receiving from said content server, A procedure of making contents of pay service downloading from said content server, When download of contents of said pay service is unsuccessful, said permission ID is used, A program for pay service offer making said terminal perform again a procedure of making a download request of contents of

said pay service requiring from said content server.
[Claim 14]The program for pay service offer according to claim 13 having a procedure of making contents of said enciphered pay service made downloading from said content server decrypting using said operation information for attestation as a common key.
[Claim 15]A terminal and a content server which provides contents to said terminal, . A prepaid information management server which performs accounting of pay service can set to a pay service provision system connected to a network. A procedure to which are a program for pay service offer which controls said content server, and a service menu is made to transmit to said terminal based on a demand from said terminal, From said terminal, said prepaid information management server is received according to a demand using prepaid information media holding predetermined information required for dealings of use of pay service, Attestation of whether to have the qualification for said prepaid information media using pay service of said contents, A procedure of making fee collection to said prepaid information media requiring, and a procedure of making contents of said pay service providing to said terminal based on a completion notification of attestation from said prepaid information management server, and fee collection, Said permission ID is used from a means which generates permission ID which validates download of contents of said pay service in the range within a fixed limit based on a completion notification of attestation from said prepaid information management server, and fee collection, and is made to transmit to said terminal, and said terminal, A program for pay service offer making a content server perform a procedure of making contents of said pay service providing in said fixed limit, to said terminal when a download request of contents of said pay service occurs again.
[Claim 16]The program for pay service offer according to claim 15 provided with a procedure of making contents of said pay service enciphering by using as a common key operation information for attestation received from said prepaid information management server, and making said terminal providing with contents of said pay service.
[Claim 17]A terminal and a content server which provides contents to said terminal, . A prepaid information management server which performs accounting of pay service can set to a pay service provision system connected to a network. Attestation of whether to have the qualification for being a program for pay service offer which controls said prepaid information management server, and said prepaid information media from said content server using pay service of said contents, Said terminal is

received based on a demand of fee collection to said prepaid information media, A procedure of making transmission of prepaid use ID stored in said prepaid information media requiring, A procedure to which operation information for attestation is made to transmit to said terminal after receiving the prepaid use ID concerned, After receiving the result of an operation which performed a predetermined operation to a password of said prepaid information media using said operation information for attestation from said terminal, A procedure of performing the same operation as an operation which said terminal used for said password of said prepaid information media stored in a database using said operation information for attestation, comparing the result of an operation with the result of an operation to which it was transmitted from said terminal, and making said prepaid information media attesting, A procedure of searching a database based on said prepaid use ID, and making accounting performing with reference to said charge request amount of money from the balance and said content server of prepaid information media of the prepaid use ID concerned, Said terminal is received when both said attestation and said accounting are successful, completion information of pay service use procedure, and information containing the balance of prepaid information media -- a program for pay service offer making said prepaid information management server perform a procedure to which a completion notification of attestation and fee collection is made to transmit to said content server.

[Claim 18]The program for pay service offer according to claim 17 having a procedure to which said operation information for attestation of said prepaid information is made to transmit to said content server.

[Claim 19]A recording medium which stored the program for pay service offer according to any one of claims 13 to 18 and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention A pay service provision method, a pay service provision system, a content server, With respect to a pay service distribution program and a recording medium, especially, using media, such as a prepaid IC card, when a terminal is safely and certainly provided with pay content via the Internet, it is related with effective technology.

[0002]

[Description of the Prior Art]When it provides a terminal with the contents of pay service via the Internet from a content server, After receiving pay content in a terminal, in view of it being difficult to charge, two kinds of methods shown below are known as a collecting method of the charge of such pay content.

(1) One of them is the margin transaction using a common credit card.

(2) others -- one is a method by prepaid one.

However, when a common credit card was used, there was a problem that the deposit balance needed the member procedure to a card issuer and to be managed, and there was danger of tapping by moreover a credit number flowing on a network. On the other hand, those who do not own a credit card also have a method by prepaid one, and the feature of being available as the example, For example, JP,H11-316729,A ("recording medium which recorded the internet charging method/system and the Internet accounting program") is known.

[0003]Below, invention (henceforth precedence invention) indicated by JP,H11-316729,A is explained in detail as a conventional example of the method by prepaid one. those who do not own a credit card being also available, and precedence invention, Drawing 8 explains the outline of operation of precedence invention for the purpose of providing the recording medium which stored the internet charging method/system and the Internet accounting program which can be eliminated certainly for the order which is not desirable. first, a prepaid card (an IC card and a floppy (registered trademark) disk.) Based on the address information (for example, URL in HTTP) of the content server set to the magnetic card etc., a pay service utilization request is published from a terminal to a content server (Step 101). Next, it is required for a card management server that a content server should perform attestation and accounting of a prepaid card (Step 102). Next, a card management server attests a card between terminals (Step 103), and returns attestation and an accounting result to a content server (Step 104). Next, a content server provides pay service for a terminal, when attestation and accounting are successful (Step 105).

[0004]Drawing 9 is a block diagram showing the outline of the connection configuration of precedence invention. The terminal 100 sets up the connection (connection for service start requests) 11 between the content servers 200 via the Internet 400, and requires use of pay service using the connection 11 concerned. If the pay service utilization request from the terminal 100 is received, the content server 200, Set up the connection (fee collection and connection for authentication demands) 12 between the card management servers 300, and the connection 12 concerned is used, By transmitting the IP address (Internet Protocol Addres) of the terminal 100,

the authentication demand of a prepaid card and an accounting demand are performed. If the authentication demand from the content server 200 is received, the card management server 300 will set up the connection (connection for authenticating processings) 13 between the terminals 100, and will require the operation of the password of a prepaid card from the terminal 100. The terminal 100 transmits the result of an operation of a password to the card management server 300 using the connection 13.

[0005]The card management server 300 holds the card identity child (henceforth card ID) of each card, the password, and the card management database (henceforth the card management DB) 500 that memorized service use point residual frequency. The card management server 300 searches a password from card ID, and if the same operation as the terminal 100 is performed and it is in agreement with the sent result of an operation, it will be taken as attestation formation. The card management server 300 notifies an authentication result and an accounting result to the content server 200 after authenticating processing and the end of accounting. When authenticating processing and accounting are materialized, the content server 200 starts offer of the contents of pay service to the terminal 100. When authenticating processing or accounting is not materialized, the content server 200 reports that a card is unusable to the terminal 100 using the connection 11.

[0006]Drawing 10 is a block diagram showing the outline system configuration of precedence invention. The terminal 100 which requires use of the pay service which accesses the content server 200 based on the contents server address information set as the prepaid card, and the content server 200 provides, In response to the demand from the content server 200 which provides pay service to the terminal 100 in response to the demand from the terminal 100 concerned, and the content server 200, it comprises attestation of a prepaid card, and the card management server 300 which performs fee collection to a prepaid card.

[0007]The terminal 100 has the service request part 101 and the card management department 102. Based on the contents server address information, including URL etc., set as the prepaid card, between the content servers 200, the service request part 101 establishes a connection automatically, and requires use of pay service. The service request part 101 can consist of WWW browsers, for example. The card management department 102 is connected with the prepaid card 103 via the reader according to the form of the prepaid card, The function which transmits card ID stored in the prepaid card based on the demand from the card management server 300, The function which transmits to the card management server 300 after reading the extra

sensitive information (password etc.) stored in the prepaid card based on the demand from the card management server 300 and, performing data processing by a tropism function etc. on the other hand, Based on the demand from the card management server 300, it has a function which writes the prepaid card balance and use time in a prepaid card.

[0008]The content server 200 has the authentication demand part 201, the accounting demand part 202, the service provision section 203, and the card management department 204. When the utilization request of pay service occurs from the terminal 100, the authentication demand part 201, Having a function in which a prepaid card performs the authentication demand of being a right thing to the card management server 300, the accounting demand part 202 has the function to require the fee collection to a prepaid card from the card management server 300. Both the service provision sections 203 have the function to provide pay service to the terminal 100 when authenticating processing and accounting are successful, and the card management department 204 has the function to require attestation of a prepaid card, and fee collection from the authentication demand part 201 and the accounting demand part 202.

[0009]The card management server 300 has the authentication section 301, the accounting part 302, and card management DB500, and the authentication section 301 has a function which attests a prepaid card to the terminal 100, when the authentication demand from the content server 200 occurs. The accounting part 302 has the function to carry out accounting according to the use degree of pay service to a prepaid card, and a function which notifies the balance of a prepaid card, and use time to the terminal 100. Card management DB500 is recording card ID of each card, a password, and service use point residual frequency.

[0010]The system action sequence in precedence invention is shown indrawing 11. The Challenge Response system which is prescribed by distribution of Video as pay service and is here specified by RFC1334 as an authentication method (W.) [Simpson and] It explains using "PPPCha11enge Handshake Authentication Protoco1 (CHAP)" and the example which uses Aug 1996. Introduction and the terminal 100 set up a connection between the content servers 200 which have the address concerned using the contents server address information (for example, URL) set as the prepaid card, and require a service menu (Step 201). Next, setting out of a connection will transmit service menus, such as a list of Video, from the content server 200 (Step 202). Next, selection of the service which a user wants to use will transmit the service utilization request message to which the service use point size required in order to use the

selected service to the content server 200 was set (Step 203).
[0011]Next, by transmitting the authentication demand message which the content server 200 set up the connection between the card management servers 300, and set up the IP address of the terminal 100 using the connection concerned, A prepaid card performs the authentication demand of being a right prepaid card to the card management server 300 (Step 204). Accounting is required by transmitting simultaneously the accounting request message which set up the service frequency of use service to the card management server 300. Even if they are the same message, and an authentication demand message and an accounting request message are separate messages, they are feasible. Next, the card management server 300sets up a connection between the terminals 100 based on the IP address of the terminal 100 in the authentication demand message which received, and requires card ID of the terminal 100 using the connection concerned (Step 205).
[0012]Next, the terminal 100 transmits card ID stored in the prepaid card to the card management server 300 (Step 206). Next, the card management server 300 transmits the random number for attestation (challenge) to the terminal 100 using the connection set up between the terminals 100 (Step 207). A value which is different whenever this random number attests the terminal 100 is used. next -- as opposed to the value with which the terminal 100 which received the random number combined the random number and the password -- MD5n (RivestR and S. --) [Dusse and] Response messages which calculated with the tropism function on the other hand, and set up the result (response), such as "The MD5 Message-Digest Algorithm" and April1992, are transmitted to the card management server 300 (Step 208).
[0013]Next, while the card management server 300 is as the same as the terminal used it to the value which unified the password of the prepaid card currently held to card management DB500, and the random number which transmitted to the terminal 100, it calculates by a tropism function, and it compares the result with the response from the terminal 100. If both are in agreement, I will consider it as attestation formation (Step 209), and both will - Do, and if there is nothing, it will be considered as attestation failure. Thus, since random numbers different each time are used for attestation of a card, even if a third party intercepts a challenge and a response, at the time of the next attestation, using the value, the card management server 300 becomes a user of the terminal 100, and cannot be cleared up. The original password cannot be presumed though the 3rd person can know a response, since the operation value by a tropism function is used for a response on the other hand.
[0014]Next, the card management server 300 searches card management DB500

based on card ID, and if the residual frequency of the service use point of an applicable card is larger than the service point set as the accounting request message, Only the number of service points set as the accounting request message subtracts the service use point of an applicable card (Step 210). If the residual frequency of the service use point of an applicable card is smaller than the service point set as the accounting request message, accounting will be made impossible and processing will be ended. Processing is ended when attestation and accounting are impossible. Next, the card management server 300 notifies the balance of a prepaid card, and use time to the terminal 100 (Step 211), and notifies attestation and an accounting result to the content server 200 (Step 212). Finally, the content server 200 provides pay service to the terminal 100 (Step 213).

[0015]Drawing 12 is a flow chart which shows the procedure of the terminal 100 of precedence invention. Hereafter, the procedure of the terminal 100 is explained using drawing 12. First, based on the address information currently recorded on the prepaid card, a connection is set up between the content servers 200, and a service menu is required from the content server 200 (Step 301). Next, the service utilization request message to which the necessary point size of service was set is transmitted to the content server 200 using the set-up connection (Step 302). Next, based on the demand from the card management server 300, card ID stored in the prepaid card is transmitted to the card management server 300 (Step 303).

[0016]Next, after reading the extra sensitive information (password etc.) stored in the prepaid card based on the demand from the card management server 300 and, performing data processing by a tropism function etc. on the other hand, it transmits to the card management server 300 (Step 304). When attestation and fee collection are successful, the balance is notified from the card management server 300 (Step 305), and offer of the contents of pay service can be received (Step 306). The value of the balance notified from the card management server 300 is displayed on the terminal 100, and it can write the balance and use time in a prepaid card. Pay service is not provided when attestation or fee collection goes wrong (Step 307).

[0017]Drawing 13 is a flow chart which shows the procedure of the content server of precedence invention. Hereafter, the procedure of a content server is explained using drawing 13. First, if there is a demand of a service menu from the terminal 100, a service menu list will be transmitted to the terminal 100 (Step 401), and a pay service utilization request will be received from the terminal 100 (Step 402). To the card ID part of attestation and a charge request message at card ID and a terminal address part Next, a terminal address, Attestation of a card and the fee collection to a

card are required from the card management server 300 by setting up the necessary point size of the service used for a service point part, respectively, and transmitting the message concerned to the card management server 300 (Step 403). In this example, in order that the card management server 300 may require card ID of the terminal 100, card ID does not set up.

[0018]However, there are a method of transmitting card ID, when transmitting a pay service demand to the content server 200 from the terminal 100, and a way the terminal 100 transmits card ID to the content server 200 based on the demand from the content server 200, as other examples. Card ID is set up in these cases. Next, it judges whether attestation and fee collection were materialized (Step 404), and, in YES, offer of the contents of pay service is started to the terminal 100 at Step 404 (Step 405). In NO, it is reported at Step 404 that attestation or accounting was not materialized to the terminal 100 (Step 406).

[0019] Drawing 14 is a flow chart which shows the procedure of the card management server of precedence invention. Hereafter, the procedure of the card management server 300 is explained using drawing 14. First, the attestation and the charge request message from the content server 200 are received (Step 501). When card ID is not set as the message concerned, Based on the IP address of the terminal 100 in the attestation and the charge request message which received, a connection is set up between the terminals 100, and card ID is required of the terminal 100 using the connection concerned (Step 501-1). When card ID is set as the message concerned, the random number for attestation (challenge) is transmitted to the terminal 100 (Step 502). A value which is different whenever this random number attests the terminal 100 is used. In this case, when the connection is not set up between the terminals 100, Based on the IP address of the terminal 100 in the attestation and the charge request message which received, a connection is set up between the terminals 100, and the random number for attestation (challenge) is transmitted to the terminal 100 using the connection concerned.

[0020]Next, receive the response (response) from the terminal 100 and the value which unified the password of the prepaid card currently held by card management DB500 and the random number which transmitted to the terminal 100 is received, Authenticating processing is performed by [as the terminal used it / same] calculating by a tropism function on the other hand, and comparing the result with the response from the terminal 100 (Step 503). Next, it judges whether both were in agreement (Step 504), and, in NO, processing is ended as attestation failure at Step 504. In YES, it is judged at Step 504 whether it can charge or not (Step 505). That is,

the residual frequency of the service use point of an applicable card is compared with the service point set as the accounting request message.

[0021]At Step 505, if the residual frequency of the service use point of an applicable card is larger than the service point set as the accounting request message, Only the service point set as the accounting request message subtracts the service use point residual frequency of an applicable card (Step 506). Next, to the terminal 100, the balance of a prepaid card and use time are notified (Step 507), and attestation and an accounting result are notified to the content server 200 (Step 508). Since it cannot charge at Step 505 if the residual frequency of the service use point of an applicable card is smaller than the service point set as the accounting request message, processing is ended.

[0022]In the above-mentioned explanation, it cannot be overemphasized that the method except having mentioned above may be used as an authentication method. As pay service to provide, download of the data of a program etc., on-line shopping, etc. occur in addition to distribution of Video. The user itself may be made to enter a password, without making it build in a card. In the above-mentioned procedure, after attestation is successful, a content server is able to have composition which requires accounting of a card management server, and the amount of money, and a point and other arbitrary forms are possible as a further prepaid form.

[0023]

[Problem to be solved by the invention]As mentioned above, since the pay service demand from a terminal is received only when the authenticating processing and accounting of a prepaid card are completed correctly, by a conventional example, the order which is not desirable can be eliminated certainly. In precedence invention, the content server 200 transmits the address information of the terminal 100 to the card management server 300, accesses the terminal 100 directly from the card management server 300, and can attest the prepaid card on a terminal. Therefore, it can prevent certainly revealing to a content server with inaccurate extra sensitive information of the password of a prepaid card, etc. However, since pulling down fee collection is performed before the pay information distribution from the content server 300, After canceling the connection of the terminal 100 and the content server 200, when it turned out that contents were not able to download normally, the terminal 100 had the problem that a means to access a content server was not left behind.

[0024]This problem is a problem which may be easily produced also in use by mobile environment. As invention which solves such a problem, there is JP,2000-270309,A "fee collection to distribute information, adjustment system, and its server." In

JP,2000-270309,A, after a server charges directly a content rate which should be downloaded to a terminal to a prepaid charge, it downloads pay information to a terminal, investigates the amount of information which a terminal received by download, and sends receiving quantities to a server. A server is a system which measures a transmission amount and receiving quantities, judges that reception did not go well when both are inharmonious, and repays the phase present. According to this system, there is a problem that only refund of a rate of a constant ratio will be made also to meaningless contents if the whole is not received, and it can become meaningless even if it carries out complicated control.

[0025]Are made in order that this invention may solve a problem of said conventional technology, and the purpose of this invention, Those who do not own a credit card in a pay service provision method and a pay service provision system are also available, It is in providing technology it becomes possible it not only to be able to to eliminate certainly order which is not desirable, but to also enable normal download of pay content and to prevent unjust download. Other purposes of this invention are to provide a content server used for the above-mentioned pay service provision system. Other purposes of this invention are to provide a control program which makes a computer perform the above-mentioned pay service provision method. Other purposes of this invention are to provide a recording medium with which the above-mentioned program was recorded. The other purposes and the new feature are clarified with description and an accompanying drawing of this Description along [said] this invention.

[0026]

[Means for solving problem]It will be as follows if the outline of a typical thing is briefly explained among invention indicated in an application concerned. Namely, this invention is a pay service provision method, and a content server, When permission ID which validates download of the contents of pay service in the range within a fixed limit is generated, it transmits to a terminal and a terminal is not able to receive the contents of pay service normally, above-mentioned permission ID is used, It was repeatedly presupposed that it is accessible at the content server until the contents of pay service could receive normally. Thereby, even if it charges beforehand before distribution of the contents of pay service, it enables a user for the contents of pay service to come to hand certainly.

[0027]Authentication arithmetic information (.) which this invention is a pay service provision method, and the prepaid information management server which performs card authentication transmitted to the terminal for attestation of prepaid information

media Or a content server is provided with an authentication arithmetic result, and a content server is the authentication arithmetic information (.) concerned. Or the contents of pay service are enciphered, it provides for a terminal, using an authentication arithmetic result as a common key, and a terminal decrypts the provided contents which were enciphered, using the authentication arithmetic information (or authentication arithmetic result) used in the attestation stage as a common key. The contents are not understood even if the downloaded contents leak to others by this, Since it cannot decode as long as there is no common key even if persons other than a user use download permission ID improperly, it can be judged whether charged contents reached only the user certainly, and a user and both of a content server have an effect.

[0028]A password is not held in prepaid information media, such as an IC card, a floppy disk, a magnetic card, etc. which are pay service provision methods and are connected to a terminal, but a user operates a terminal, and this invention inputs it from the outside. By this, only a user who can use this password will have a right to download, and can raise the safety of prepaid information media, and a third party's unjust download can be prevented. This inventions are a pay service provision system for realizing the above-mentioned pay service provision method, and a content server. This invention is a program for pay service offer which performs control of a terminal for realizing the above-mentioned pay service provision method, a content server, and a prepaid information management server. This invention is a recording medium which stores the above-mentioned pro crumb and in which computer reading is possible.

[0029]

[Mode for carrying out the invention]Hereafter, with reference to Drawings, an embodiment of the invention is described in detail. In a complete diagram for describing an embodiment, what has the same function attaches identical codes, and explanation of the repetition is omitted. In this Description, although a user calls a prepaid card hereafter prepaid information media used when requiring service use of a content server, in this invention, prepaid information media are not limited to a form of a card. Although a prepaid information management server is hereafter called a card management server, it is not limited to card management. A card management company publishes and manages a prepaid card, for example, and a user purchases a prepaid card, in order to use pay service. Contents server address information, card ID, a card password, etc. are set to a prepaid card, and a prepaid information management server, i.e., a card management server, has managed the balances (the

amount of money or a point) of available service according to purchased amount.
[0030]This invention is improved so that the dishonesty prevention can be performed, while a user can obtain pay content for precedence invention (invention given in JP,H11-316729,A) certainly. Therefore, since its system configuration is the same as precedence invention which shows drawing 10 a pay service provision system of an embodiment of the invention, explanation of a system configuration of a pay service provision system of this embodiment is omitted. Drawing 1 is a sequence chart for explaining an outline of operation of a pay service provision system of an embodiment of the invention. In drawing 1, Step 104 is the same as a sequence chart of precedence invention shown in drawing 8, and Step 105 or subsequent ones differs from precedence invention. A content server gives permission of pay service offer to a terminal, when attestation and accounting are successful (Step 105). It is permitted that a terminal carries out multiple-times download within limits, such as fixed time, and a content server provides pay information (Step 106,107).
[0031]Drawing 2 is a block diagram showing the outline of the connection configuration of an embodiment of the invention, and the connection 14 differs from the connection configuration of precedence invention shown in drawing 9in the figure. The terminal 100 is a connection in the case of requiring download access of the content server 200, and this connection 14 may be stretched after other connections (11-13) are released. The composition of the pay service provision system of this embodiment, The point that a download request can be performed within fixed restriction is different from precedence invention until the service request part 101 of the terminal 100 receives download ID of the contents of pay service from the content server 200 and can receive certainly using the download ID. When enciphering contents, a function is given to the service provision section 203 of the content server 200, and the service request part 101 of the terminal 100, but others are the same as that of precedence invention. Although this drawing 2explained the case where the Internet was used, as a network which connects the terminal 100, the content server 200, and the card management server 300, Public network networks which connect the terminal 100, the content server 200, and the card management server 300, such as a telephone line general as a network, are also usable.
[0032]Next, an example of a series of operations of a pay service provision system of this embodiment is concretely explained using drawing 3. Drawing 3is a sequence chart for explaining an example of a series of operations in a pay service provision system of this embodiment. In drawing 3, since Step 212 is the same as a sequence chart of precedence invention shown in drawing 11, it omits explanation and only a

point of difference explains it. The content server 200 From the card management server 300 to service provision permission. If (namely, attestation and an accounting result) are notified (Step 212), ID which permits download access of contents of pay service under fixed restriction to the terminal 100 is provided (Step 214), next pay service is provided to the terminal 100 (Step 213). the same contents for which this permission ID placed an order with effective "bottom of restriction" -- less than fixed access periods (for example, less than 24 hours) -- or, Less than fixed access frequency (for example, less than 10 times) says such combination (for example, direction arrived at at any of less than 10 times or less than 24 hours, or restriction).

[0033]Although not illustrated in drawing 3, this permission ID needs to reach the terminal 100 certainly. The same ID of ** plurality is repeated and sent as such a method, and the method of checking by taking majority, the method of returning again ID which transmitted to the terminal 100 to the content server 200, and comparing it from the ** content server 200, etc. are known. In this case, in the method of **, normality can be judged at the transmitting side by the method of ** at a receiver. Pay service is provided after being able to carry out the normal reception of this permission ID. At Step 213, when pay service is not able to receive normally, a user transmits download permission ID to the content server 200 from the terminal 100 (Step 215), and downloads the contents of pay service from the content server 200 (Step 216). In this case, permission ID is within fixed restriction, checks an effective thing, and performs control which increases an access count number depending on conditions. A terminal check will be attained if it compares whether it is the same as that of URL of the terminal of an order stage.

[0034]Next, other examples of a series of operations of a pay service provision system of this embodiment are concretely explained using drawing 4. Drawing 4 is a sequence chart for explaining other examples of a series of operations in a pay service provision system of this embodiment. In drawing 4, since Step 211 is the same as a sequence chart of precedence invention shown in drawing 11, it omits explanation and only a point of difference explains it. The card management server 300 transmits service provision permission (namely, attestation and accounting result) to the content server 200, after attestation and fee collection of the terminal 100 are completed (Step 217). An example shown in drawing 4 is the point of adding an encryption key to it, and difference is carried out to an example shown indrawing 3. Certification information which the terminal 100 calculated based on a random number and it which are the information for attestation transmitted to the terminal 100 at Step 207 from the card management server 300 as an encryption key can be used. From it being

the information which has also already held the terminal 100, these can be used as a common key, when decrypting.

[0035]Next, the content server 200 enciphers contents with the encryption key sent from the card management server 300 (Step 218). Next, the content server 200 provides ID which permits download access of the contents of pay service under fixed restriction to the terminal 100 (Step 214), and provides pay service to the terminal 100 (Step 213). The terminal 100 is decrypted with the common key in the terminal 100 to the contents information of the enciphered pay service downloaded from the content server 200 (Step 219). The accessing method of Steps 215 and 216 is the same as the example shown in drawing 3.

[0036]Drawing 5 is a flow chart which shows the procedure of the terminal 100 of this embodiment. Hereafter, the procedure of the terminal 100 of this embodiment is explained using drawing 5. In drawing 5, since Step 307 is the same as the procedure of the terminal 100 of precedence invention shown indrawing 12, it omits explanation and only a point of difference explains it. The step (308,309) which checks that the terminal 100 has carried out normal reception of download permission ID after the balance was notified from the card management server 300 at Step 305. As the above-mentioned step 214 described judgment of normal reception, efficiency is possible also for the terminal 100 side or the content server 200 side. Next, the contents of pay service are downloaded from the content server 200 (Step 310). In the case of mobile environment etc., in Step 310 which receives these contents, it cannot receive normally, for example.

[0037]Next, when contents are enciphered, it decrypts (Step 311). According to this embodiment, since the transient random number information used for terminal attestation is used for a common key, there is the feature that distribution of the further encryption key is unnecessary and safety is high. In this embodiment, although download of the case before service starts and the contents of pay service may have finished unsuccessful, access to the terminal 100 is Step 301, and judges whether it is access in case access to the terminal 100 is any. At Step 301, when a decision result is before service starts, processing of Steps 302-311 is performed. When the decision result in Step 301 retries download of the contents of pay service, it accesses to the content server 200 by permission ID first (Step 313). When it combines with information, including the address information of the terminal 100, etc., the content server 200 checks whether permission ID is effective and the content server 200 permits download for the second time, It shifts to processing (download processing of the contents of pay service) of Step 310 and Step 311, and that is displayed when a

permission cannot be granted (Step 314).

[0038]Drawing 6 is a flow chart which shows the procedure of the content server 200 of this embodiment. Hereafter, the procedure of the content server 200 of this embodiment is explained using drawing 6. In drawing 6, since Step 406 is the same as the procedure of the content server 200 of precedence invention shown in drawing 13, it omits explanation and only a point of difference explains it. By the case where terminal attestation is successful by the card management server 300, further, when enciphering contents, the information (for example, information used for terminal attestation) used as a common key is sent to the content server 200 from a card management server. The content server 200 receives the information sent from the card management server 300, uses this information as a common key, and enciphers contents (Step 407). The information used as a common key is information used for attestation, All are usable if sharable with the terminal 100 (for example, result etc. which were calculated with card use ID using the operation information for attestation sent to the terminal 100, or it from the card management server 300).

[0039]Next, download permission ID is generated (Step 408), this download permission ID is transmitted to the terminal 100 (Step 409), and it is judged whether in the terminal 100, download permission ID has received normally (Step 410). When it is judged that download permission ID was not able to receive normally in the terminal 100 at Step 410, Step 409 and Step 410 are repeated. When it is judged that download permission ID has received normally in the terminal 100 at Step 410, contents of pay service from the content server 200 to the terminal 100 are downloaded (Step 411). From a viewpoint of safety, although random generation of generation of permission ID in the content server 200 in Step 408 is desirable, it can also be created with an original rule on employment.

[0040]In this embodiment, although access from the terminal 100 over the content server 200 has a case of an initial stage of service, and a case of a retry of download of contents of pay service, At Step 401, it is judged whether it is a case where access to the terminal 100 over the content server 200 is any. When access from the terminal 100 is an initial stage of service, processing of Step 401 - Step 411 is performed. When access from the terminal 100 is the retry of download of contents of pay service, When permission ID judges whether it is in a limit (Step 413) and permission ID is judged to be outside of a limit at Step 413, it is notified to the terminal 100 that permission ID is invalid (Step 416). At Step 413, when permission ID is judged to be inside of a limit, information, including address information etc. of the terminal 100 which accompanies the permission ID, is read, it compares whether it is in agreement

with the terminal 100 with a demand (Step 414), and it is judged whether it is just use (Step 415). At Step 415, when attested with just use, it progresses to Step 411 and contents of pay service to the terminal 100 are downloaded. When attested with it not being just use at Step 415, it notifies attestation un-succeeding to the terminal 100 (Step 417).

[0041]Drawing 7 is a flow chart which shows procedure of the card management server 300 of this embodiment. Hereafter, procedure of the card management server 300 of this embodiment is explained using drawing 7. Indrawing 7, since Step 507 is the same as procedure of the card management server 300 of precedence invention shown in drawing 14, it omits explanation and only a point of difference explains it. Although it is the information which checks that information sent to the content server 200 is in authentication results, such as an IC card, and a range for which the prepaid balance can provide pay service in this embodiment, an encryption key is transmitted as occasion demands (Step 509). Thereby, an offer of information with the safer content server 200 becomes possible. As an encryption key, it is information sharable with the terminal 100, and there are some which were explained at the above-mentioned step 407. If it delivers again anew, other common keys and public keys can also be used.

[0042]As explained above, according to this embodiment, those who do not own a credit card are also available in pay information (contents of pay service), Even when an offer of information does not go well after fee collection, even if there are faults, such as user environment, by giving a user a right which can carry out repeat execution of the download, it becomes possible for information to come to hand certainly. Although there is a risk of being used also for a user besides a contract by allowing a retry of download in an information provider's position, It is effective in the ability to suppress an unauthorized use to the minimum by using together an address and permission ID of the terminal 100, and also validating within the limits of combination, such as a period and access frequency.

[0043]In the above-mentioned explanation, it cannot be overemphasized that an authentication method except having mentioned above may be used as an authentication method. As pay service to provide, in addition to distribution of Video, download of data of a program etc., on-line shopping, etc. occur, and there are an IC card, a floppy disk, a magnetic card, etc. as real original form voice of a prepaid card. The user itself may be made to enter a password, without making it build in a card. In the above-mentioned procedure, after attestation is successful, the content server 200 is able to have composition which requires accounting of the card management server

300. As a prepaid form, the amount of money, and a point and other arbitrary forms are possible.

[0044]Although balance information may be recorded on a prepaid card, in this embodiment. Since it is processed based on balance information managed by the card management server 300, if it manages unitary on the card management server 300, a risk of disagreement of balance information arising can be avoided without performing writing of prepaid KADOHE. When it becomes impossible for the 3rd person to get to know the balance easily and he does not record a password in particular in a card in the time of disasters, such as a theft of a prepaid card, by doing in this way, there is an advantage that the effect is remarkable. It cannot be overemphasized that change and application are variously possible within Claims without limiting this invention to the above-mentioned working example.

[0045]In the above-mentioned explanation, although application of prepaid KADOHE was mainly explained, This invention Not only my ledge card of an airline but a department store, a hotel, It is applicable to a settlement system using a point card currently used in the broad industries, such as soft sale (CDs, videos, game software, etc.), video, CD rental and a supermarket, household appliance sale, and a gas station. In this invention, it is similar with user ID in a membership service with a point which uses ID to which download was accepted. Once it becomes a member in a membership service in many cases, treatment of he being hardly conscious of the period, and recording each access frequency is unnecessary.

[0046]However, a user since permission ID which validated download of the contents of pay service within the fixed limit is used in this invention, It differs in that a means to manage the limit for access frequency, duration of service, etc. for each goods of every is required, and it can be considered that the guarantee of the right that what the user purchased and paid the price can be obtained certainly is given. Performing such management has guaranteed making the risk of the unauthorized use of permission ID also for a vendor into the minimum. Especially in the example shown in drawing 4, using the information which carried out terminal attestation, since contents are enciphered, there is the feature that information cannot be easily obtained even if it uses permission ID unjustly. As mentioned above, as for this invention, although invention made by this invention person was concretely explained based on said embodiment, it is needless to say for it to be able to change variously in the range which is not limited to said embodiment and does not deviate from the summary.

[0047]

[Effect of the Invention]It will be as follows if the effect acquired by the typical thing

among invention indicated in an application concerned is explained briefly.
(1) According to this invention, while it is [contents / those who do not own a credit card, or / of pay service] available, even when an offer of information does not go by faults, such as user environment, well after fee collection, it becomes possible for information to come to hand certainly.
(2) According to this invention, it becomes possible by using the address and permission ID of a terminal together, and also being effective within the limits of combination, such as a period and access frequency, to suppress an unauthorized use to the minimum.

DESCRIPTION OF DRAWINGS

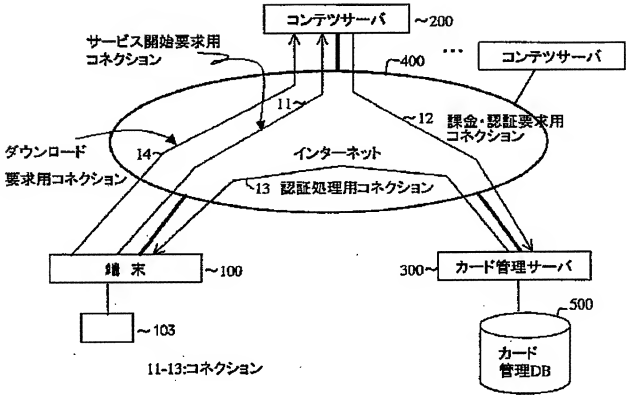
[Brief Description of the Drawings]
[Drawing 1]It is a sequence chart which shows the outline of operation of the pay service provision system of an embodiment of the invention.
[Drawing 2]It is a block diagram showing the outline of the connection configuration of the pay service provision system of an embodiment of the invention.
[Drawing 3]It is a sequence chart for explaining an example of a series of operations in the pay service provision system of this embodiment.
[Drawing 4]It is a sequence chart for explaining other examples of a series of operations in the pay service provision system of this embodiment.
[Drawing 5]It is a flow chart which shows the procedure of the terminal of an embodiment of the invention.
[Drawing 6]It is a flow chart which shows the procedure of the content server of an embodiment of the invention.
[Drawing 7]It is a flow chart which shows the procedure of the card management server of an embodiment of the invention.
[Drawing 8]It is a sequence chart which shows the outline of operation of the pay service provision system of precedence invention.
[Drawing 9]It is a block diagram showing the outline of the connection configuration of the pay service provision system of precedence invention.
[Drawing 10]It is a block diagram showing the system configuration of the pay service provision system of precedence invention.
[Drawing 11]It is a sequence chart for explaining a series of operations in the pay service provision system of precedence invention.
[Drawing 12]It is a flow chart which shows the procedure of the terminal of

precedence invention.
[Drawing 13]It is a flow chart which shows the procedure of the content server of precedence invention.
[Drawing 14]It is a flow chart which shows the procedure of the card management server of precedence invention.
[Explanations of letters or numerals]
11 -- The object for service start requests and the connection for download, 12 -- Fee collection and the connection for authentication demands, 13 -- The connection for authenticating processings, 14 -- The connection for download requests, 100 [-- Prepaid card,] -- A terminal, 101 -- A service request part, 102 -- A card management department, 103 200 [-- A service provision section, 204 / -- A card management department, 300 / -- A card management server, 301 / -- An authentication section, 302 / -- An accounting part, 400 / -- The Internet, 500 / -- Card management DB.] -- A content server, 201 -- An authentication demand part, 202 -- An accounting demand part, 203

DRAWINGS

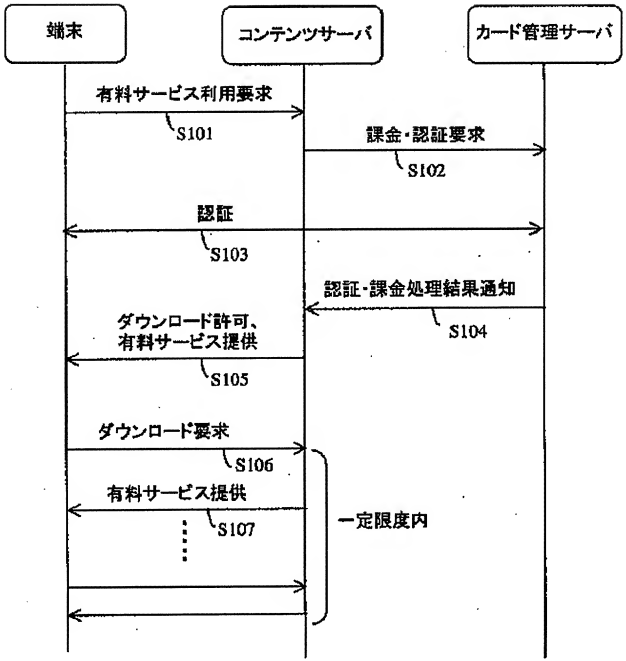
[Drawing 2]

図 2



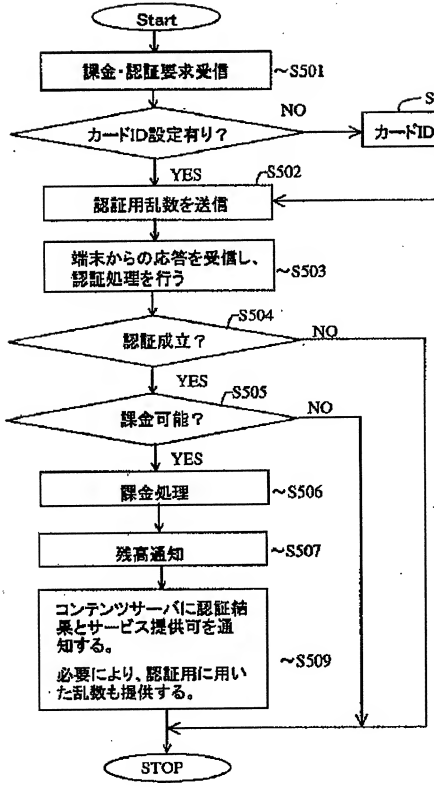
[Drawing 1]

図 1


端末
コンテンツサーバ
カード管理サーバ
有料サービス利用要求
S101
課金・認証要求
S102
認証
S103
認証・課金処理結果通知
S104
ダウンロード許可、
有料サービス提供
S105
ダウンロード要求
S106
有料サービス提供
S107
一定限度内

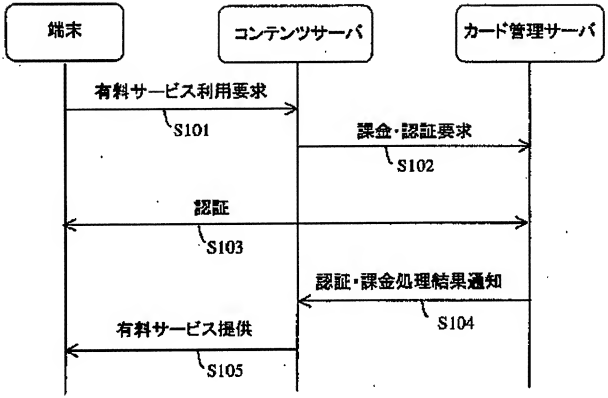
[Drawing 7]

図 7


Start
課金・認証要求受信
~S501
カードID設定有り？
NO
S501-1
カードID要求、受信
YES
S502
認証用乱数を送信
端末からの応答を受信し、認証処理を行う
~S503
S504
認証成立？
NO
YES
S505
課金可能？
NO
YES
課金処理
~S506
残高通知
~S507
コンテンツサーバに認証結果とサービス提供可を通知する。
必要により、認証用に用いた乱数も提供する。
~S509
STOP

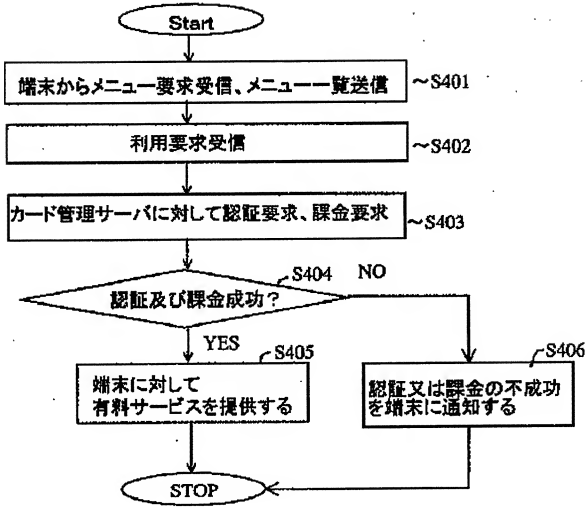
[Drawing 8]

図 8



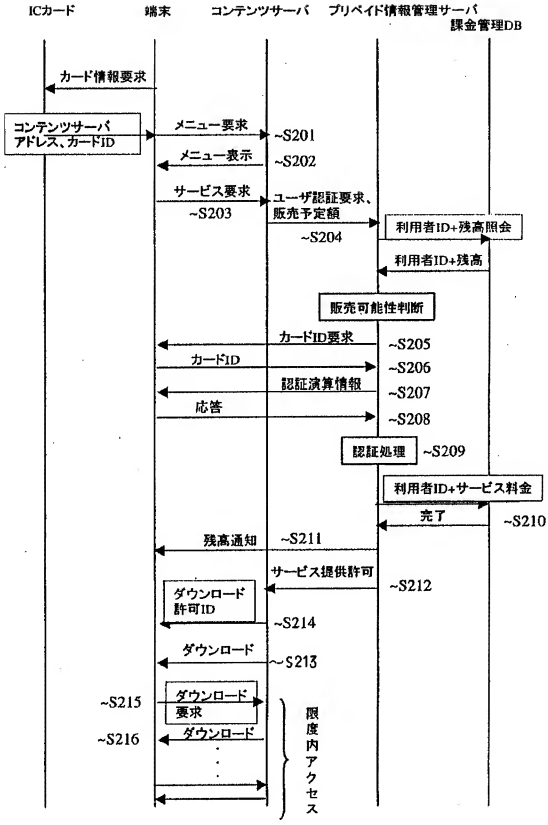
[Drawing 13]

図１３



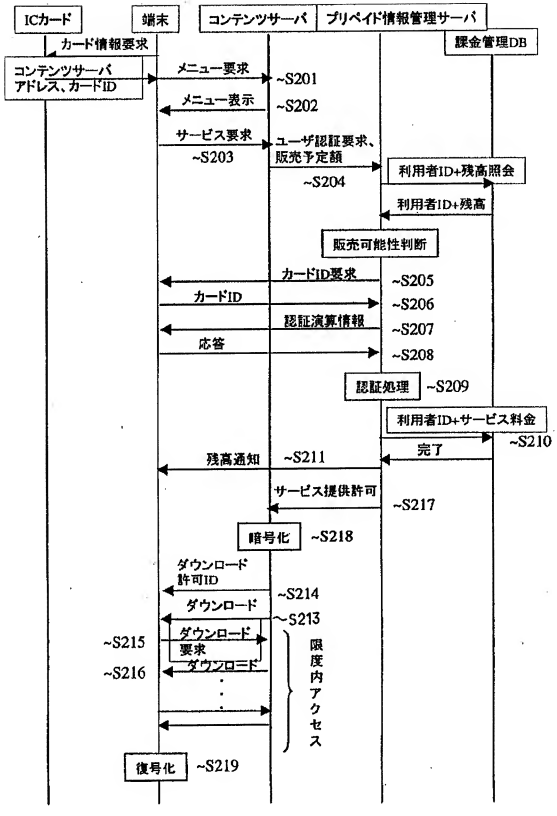
[Drawing 3]

図 3


ICカード
端末
コンテンツサーバ
プリペイド情報管理サーバ
課金管理DB
カード情報要求
コンテンツサーバ
アドレス、カードID
メニュー要求
~S201
メニュー表示
~S202
サービス要求
~S203
ユーザ認証要求、
販売予定額
~S204
利用者ID+残高照会
利用者ID+残高
販売可能性判断
カードID要求
~S205
カードID
~S206
認証演算情報
~S207
応答
~S208
認証処理
~S209
利用者ID+サービス料金
完了
~S210
残高通知
~S211
サービス提供許可
~S212
ダウンロード
許可ID
~S214
ダウンロード
~S213
~S215
ダウンロード
要求
~S216
ダウンロード
限度内アクセス

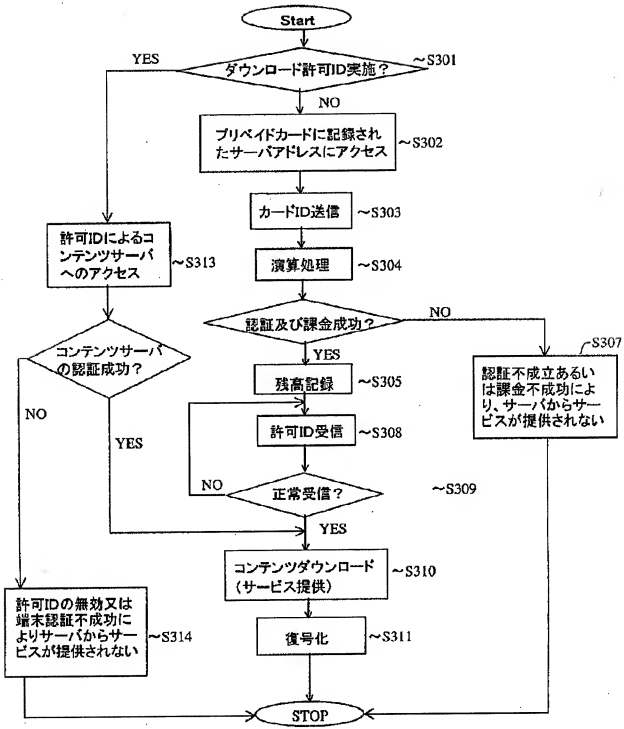
[Drawing 4]

図4


ICカード
端末
コンテンツサーバ
プリペイド情報管理サーバ
課金管理DB
カード情報要求
コンテンツサーバ
アドレス、カードID
メニュー要求
~S201
メニュー表示
~S202
サービス要求
~S203
ユーザ認証要求、
販売予定額
~S204
利用者ID+残高照会
利用者ID+残高
販売可能性判断
カードID要求
~S205
カードID
~S206
認証演算情報
~S207
応答
~S208
認証処理
~S209
利用者ID+サービス料金
~S210
完了
残高通知
~S211
サービス提供許可
~S217
暗号化
~S218
ダウンロード
許可ID
~S214
ダウンロード
~S213
~S215
ダウンロード
要求
~S216
ダウンロード
限度内アクセス
復号化
~S219

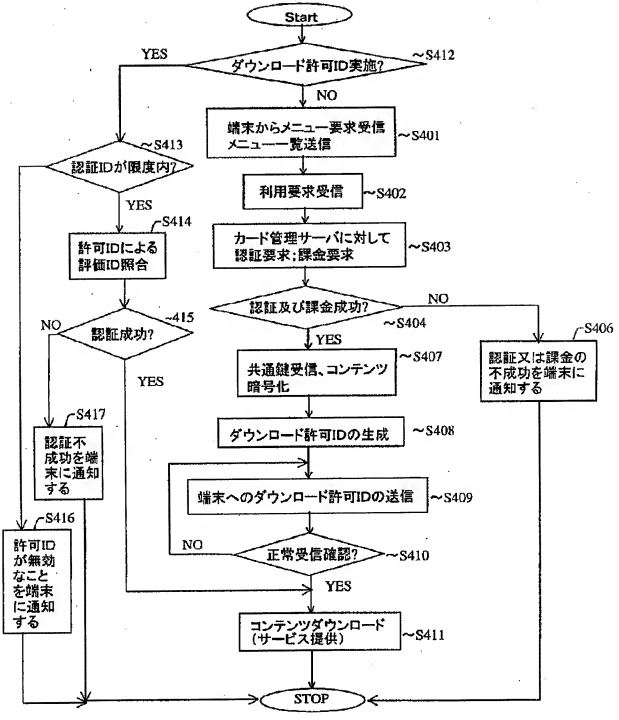
[Drawing 5]

図 5


Start
ダウンロード許可ID実施？
S301
YES
NO
プリペイドカードに記録されたサーバアドレスにアクセス
S302
カードID送信
S303
演算処理
S304
認証及び課金成功？
NO
YES
S307
認証不成立あるいは課金不成功により、サーバからサービスが提供されない
残高記録
S305
許可ID受信
S308
正常受信？
S309
NO
YES
コンテンツダウンロード（サービス提供）
S310
復号化
S311
許可IDによるコンテンツサーバへのアクセス
S313
コンテンツサーバの認証成功？
NO
YES
許可IDの無効又は端末認証不成功によりサーバからサービスが提供されない
S314
STOP

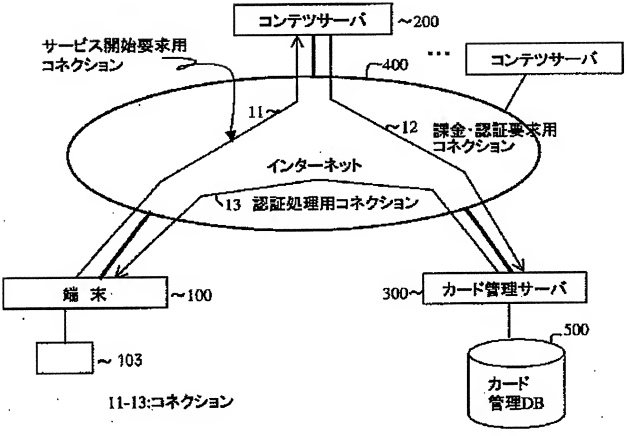
[Drawing 6]

図 6



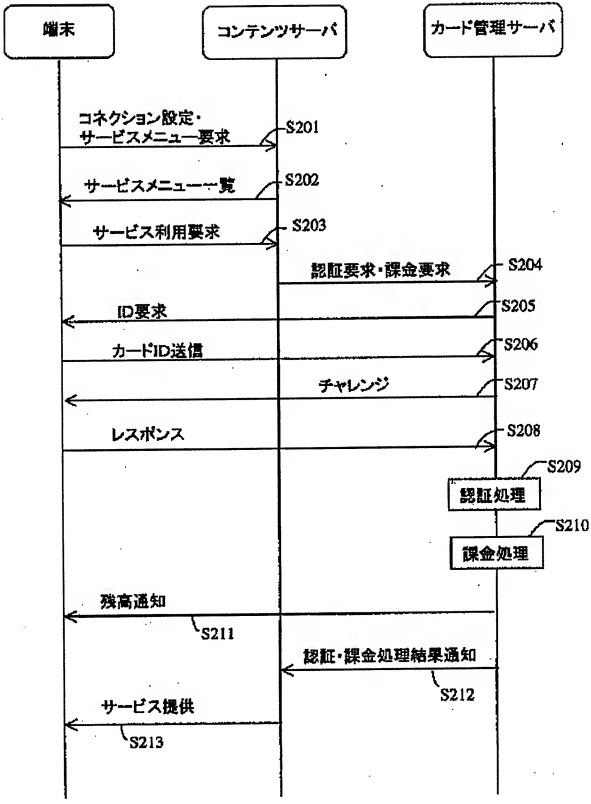
[Drawing 9]

図 9



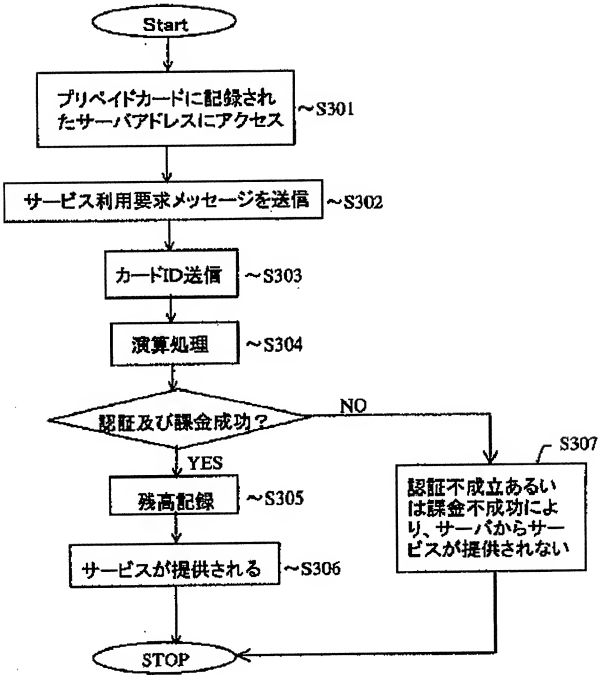
[Drawing 11]

図１１


端末
コンテンツサーバ
カード管理サーバ
コネクション設定・
サービスメニュー要求
S201
サービスメニュー一覧
S202
サービス利用要求
S203
認証要求・課金要求
S204
ID要求
S205
カードID送信
S206
チャレンジ
S207
レスポンス
S208
S209
認証処理
S210
課金処理
残高通知
S211
認証・課金処理結果通知
S212
サービス提供
S213

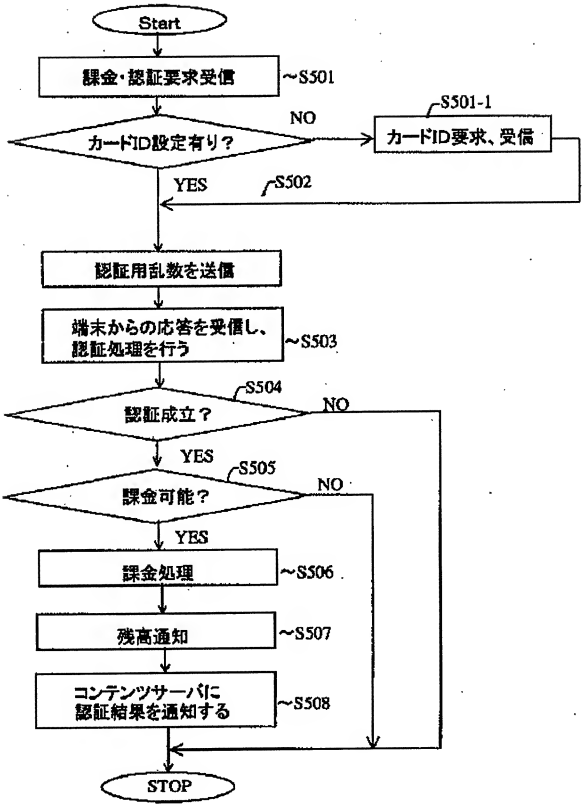
[Drawing 12]

図１２



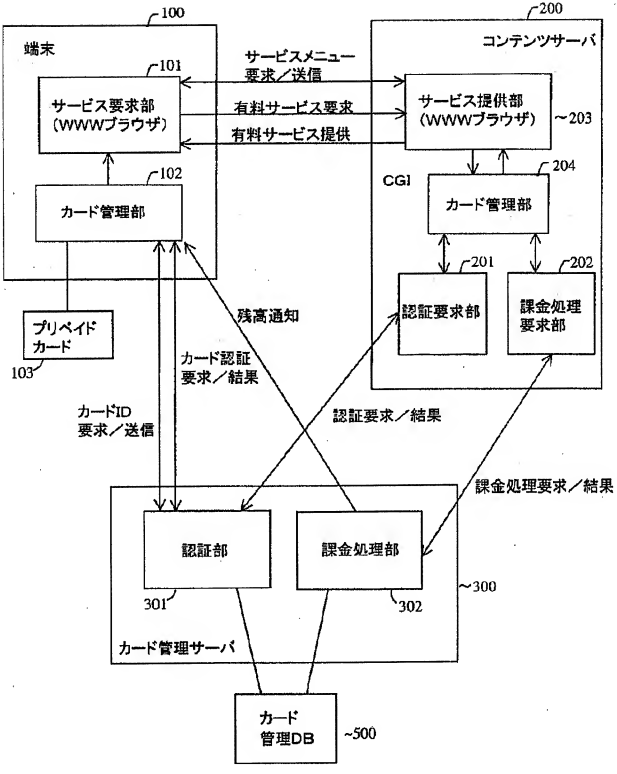
[Drawing 14]

図１４


Start
課金・認証要求受信
~S501
カードID設定有り？
NO
S501-1
カードID要求、受信
YES
S502
認証用乱数を送信
端末からの応答を受信し、
認証処理を行う
~S503
認証成立？
S504
NO
YES
課金可能？
S505
NO
YES
課金処理
~S506
残高通知
~S507
コンテンツサーバに
認証結果を通知する
~S508
STOP

[Drawing 10]

図１０


100
端末
101
サービス要求部
(WWWブラウザ)
102
カード管理部
プリペイド
カード
103
サービスメニュー
要求／送信
有料サービス要求
有料サービス提供
200
コンテンツサーバ
サービス提供部
(WWWブラウザ)
~203
CGI
204
カード管理部
201
認証要求部
202
課金処理
要求部
残高通知
カード認証
要求／結果
カードID
要求／送信
認証要求／結果
課金処理要求／結果
認証部
課金処理部
301
302
~300
カード管理サーバ
カード
管理DB
~500

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-334227
(43)Date of publication of application : 22.11.2002

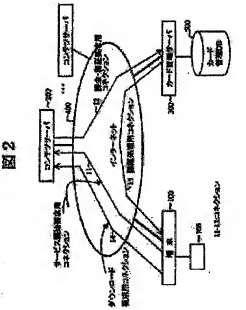
(51)Int.Cl. G06F 17/60
G06F 15/00
H04L 9/08
H04L 9/32

(21)Application number : 2001-140168
(22)Date of filing : 10.05.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SUWA YUICHI

(54) PAY SERVICE PROVISION METHOD, PAY SERVICE PROVISION SYSTEM, CONTENT SERVER, PROGRAM FOR PAY SERVICE PROVISION, AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a pay service provision method which is available even for a person not owning a credit card and can surely provide pay contents.
SOLUTION: In the pay service provision system, a terminal, a content server providing the terminal with the contents and a prepaid information management server performing the charging processing of pay services are connected to a network. The content server receives the completion report of authentication and charging from the prepaid information management server, then provides the terminal with the pay contents, generates a permission ID validating the downloading of the pay contents within a fixed limited range and transmits it to the terminal. Further, in the case that the downloading of the pay contents is requested again by using the permission ID from the terminal, the contents of the pay service are provided for the terminal within the fixed limit.



(19)日本国特許庁（ＪＰ）　　(12) **公開特許公報**（Ａ）　　(11)特許出願公開番号
特開2002－334227
（P2002－334227A）
(43)公開日　平成14年11月22日(2002.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*（参考）
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｂ０８５
	２４２		２４２	５Ｊ１０４
	３３２		３３２	
	４０８		４０８	
	４１４		４１４	

審査請求　未請求　請求項の数19　ＯＬ　（全 21 頁）　最終頁に続く

(21)出願番号　特願2001－140168(P2001－140168)

(22)出願日　平成13年５月10日(2001.5.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　諏訪　裕一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜　（外１名）

Ｆターム(参考)　5B085 AC04 AE01 AE29 BA07 BG07
5J104 AA07 AA16 EA16 KA02 KA03
KA06 MA04 NA02 NA05 NA35
NA36 PA11

(54)【発明の名称】　有料サービス提供方法、有料サービス提供システム、コンテンツサーバ、有料サービス提供用プログラム、および記録媒体

(57)【要約】
【課題】　クレジットカードを所有しない人でも利用可能で、有料のコンテンツを確実に提供することが可能な有料サービス提供方法を提供する。
【解決手段】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおいて、前記コンテンツサーバは、前記プリペイド情報管理サーバからの認証、および課金の完了通知を受け取った後に、前記端末に対して、前記有料のコンテンツを提供するとともに、前記有料のコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して前記端末に送信し、さらに、前記端末から前記許可ＩＤを用いて、再度前記有料コンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料のサービスのコンテンツを提供する。

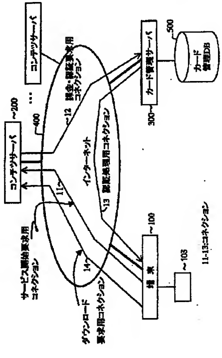


図２

1

【特許請求の範囲】

【請求項１】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおける有料サービス提供方法であって、

前記端末は、取引に必要な所定の情報を保持するプリペイド情報媒体を利用して、前記コンテンツサーバに対して前記有料サービスの利用を要求し、

前記コンテンツサーバは、前記プリペイド情報管理サーバに対して、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金とを要求し、

前記プリペイド情報管理サーバは、前記プリペイド情報媒体の認証と、前記プリペイド情報媒体に対して課金処理を行った後に、前記コンテンツサーバに対して認証、および課金の完了通知を行い、

前記コンテンツサーバは、前記プリペイド情報管理サーバからの認証、および課金の完了通知を受け取った後に、前記端末に対して、前記有料サービスのコンテンツを提供するとともに、前記有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して前記端末に送信し、さらに、前記端末から前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料サービスのコンテンツを提供することを特徴とする有料サービス提供方法。

【請求項２】　前記コンテンツサーバは、前記端末に対して、暗号化された前記有料サービスのコンテンツを提供し、

前記端末は、前記暗号化された有料サービスのコンテンツを復号化することを特徴とする請求項１に記載の有料サービス提供方法。

【請求項３】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおける有料サービス提供方法であって、

前記端末は、取引に必要な所定の情報を保持するプリペイド情報媒体を利用して、前記コンテンツサーバに対して前記有料サービスの利用を要求し、

前記コンテンツサーバは、前記プリペイド情報管理サーバに対して、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金とを要求し、

前記プリペイド情報管理サーバは、前記端末に対して、前記プリペイド情報媒体に格納されたプリペイド利用ＩＤと、前記プリペイド情報媒体のパスワードとの送信を要求し、

2

前記端末は、前記プリペイド情報管理サーバに対して、前記プリペイド利用ＩＤを送信するとともに、前記プリペイド情報媒体のパスワードを、前記パスワードを用いた所定の認証方法により認証して前記プリペイド情報管理サーバに送信し、

前記プリペイド情報管理サーバは、前記所定の認証方法で認証された前記パスワードを用いて前記プリペイド情報媒体の認証を行い、かつ、前記プリペイド利用ＩＤを基にデータベースを検索し、前記プリペイド利用ＩＤのプリペイド情報媒体の残金と前記コンテンツサーバからの前記課金要求金額を参照し、前記プリペイド情報媒体の前記残高が前記課金要求金額よりも大きいときに前記プリペイド情報媒体の前記残高に対して課金処理を行い、

前記プリペイド情報管理サーバは、前記認証と前記課金処理が共に成功した場合に、前記端末に対してプリペイド情報媒体の残高を含む情報を通知するとともに、前記コンテンツサーバに対して認証及び課金の完了通知を行い、

前記コンテンツサーバは、前記端末に対して前記有料サービスのコンテンツを提供するとともに、前記有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して、前記端末に対して送信し、さらに、前記端末において前記有料サービスのコンテンツのダウンロードが不成功に至り、前記端末から前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料サービスのコンテンツを提供することを特徴とする有料サービス提供方法。

【請求項４】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおける有料サービス提供方法であって、

前記端末は、取引に必要な所定の情報を保持するプリペイド情報媒体を利用して前記コンテンツサーバに対してサービスメニューを要求し、

前記コンテンツサーバは、前記端末に対してサービスメニューを送信し、

前記端末は、ユーザが利用するサービスを選択すると、前記コンテンツサーバに対して有料サービスの利用を要求し、

前記コンテンツサーバは、前記プリペイド情報管理サーバに対して、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金とを要求し、

前記プリペイド情報管理サーバは、前記端末に対して、前記プリペイド情報媒体に格納されたプリペイド利用ＩＤの送信を要求するとともに、前記端末に対して認証用

演算情報を送信し、
前記端末は、前記プリペイド情報管理サーバに対して前記利用ＩＤを送信するとともに、前記認証用演算情報を用いて前記プリペイド情報媒体のパスワードに対して所定の演算を行い、当該演算結果を前記プリペイド情報管理サーバに対して送信し、
前記プリペイド情報管理サーバは、データベースに格納されている前記プリペイド情報媒体の前記パスワードに対して、前記認証用演算情報を用いて、前記端末が使用した演算と同一の演算を行い、当該演算結果と前記端末から送信された演算結果と照合して前記プリペイド情報媒体の認証を行うとともに、前記プリペイド利用ＩＤを基にデータベースを検索し、当該プリペイド利用ＩＤのプリペイド情報媒体の残金と前記コンテンツサーバからの前記課金要求金額を参照し、前記プリペイド情報媒体の前記残高が前記課金要求金額よりも大きいときに前記プリペイド情報媒体の前記残高を減額する課金処理を行い、
前記プリペイド情報管理サーバは、前記認証と前記課金処理が共に成功した場合に、前記端末に対して有料サービス利用手続の完了情報とプリペイド情報媒体の残高を含む情報を通知するとともに、前記コンテンツサーバに対して、認証、および課金の完了通知と、前記認証用演算情報、あるいは前記演算結果を送信し、
前記コンテンツサーバは、前記認証用演算情報、あるいは前記演算結果を共有鍵として用い、有料サービスのコンテンツを暗号化して前記端末に提供するとともに、前記有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して前記端末に送信し、さらに、前記端末において前記有料サービスのコンテンツのダウンロードが不成功に至り、前記端末から前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料サービスのコンテンツを提供し、
前記端末は、前記認証用演算情報、あるいは前記演算結果を共有鍵として用い、前記暗号化された有料サービスのコンテンツを復号化することを特徴とする有料サービス提供方法。
【請求項５】　前記プリペイド情報媒体のパスワードは、外部から前記端末に入力されることを特徴とする請求項３または請求項４に記載の有料サービス提供方法。
【請求項６】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムであって、
前記端末は、取引に必要な所定の情報を保持するプリペイド情報媒体を利用して、前記コンテンツサーバに対して有料サービスの利用を要求する手段と、
前記コンテンツサーバから、前記有料サービスのコンテンツを受信する手段と、
前記コンテンツサーバから、前記有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを受信する手段と、
前記許可ＩＤを用いて、前記コンテンツサーバから再度前記有料サービスのコンテンツのダウンロードを要求する手段とを備え、
前記コンテンツサーバは、前記プリペイド情報管理サーバに対して、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金とを要求する手段と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記端末に対して前記有料サービスのコンテンツを提供する手段と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記許可ＩＤを生成して前記端末に送信する手段と、
前記端末から、前記許可ＩＤを用いて再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して前記一定限度内において前記有料サービスのコンテンツを提供する手段とを備え、
前記プリペイド情報管理サーバは、前記プリペイド情報媒体の認証と、前記プリペイド情報媒体の前記残高に対して課金処理を行う手段と、
前記コンテンツサーバに対して認証、および課金の完了通知を行う手段とを備えることを特徴とする有料サービス提供システム。
【請求項７】　前記コンテンツサーバは、前記端末に提供する前記有料サービスのコンテンツを暗号化する手段を備え、
前記端末は、前記暗号化された有料サービスのコンテンツを復号化する手段を備えることを特徴とする請求項６に記載の有料サービス提供方法。
【請求項８】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムであって、
前記端末は、取引に必要な所定の情報を保持するプリペイド情報媒体を利用して前記コンテンツサーバに対してサービスメニューを要求する手段と、
ユーザが利用するサービスを選択すると、前記コンテンツサーバに対して有料サービスの利用を要求する手段と、
前記プリペイド情報管理サーバに対して、前記プリペイド情報媒体に格納されたプリペイド利用ＩＤを送信する手段と、
前記プリペイド情報管理サーバから送信される認証用演算情報を受信し、前記認証用演算情報を用いて前記パスワードに対して所定の演算を行い、その演算結果を前記

プリペイド情報管理サーバに送信する手段と、
前記コンテンツサーバから、有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを受信する手段と、
前記コンテンツサーバから前記有料サービスのコンテンツを受信する手段とを備え、
前記コンテンツサーバは、前記端末にサービスメニューを送信する手段と、
前記端末のアドレス情報と前記有料サービスの課金情報とを前記プリペイド情報管理サーバに転送する手段と、
前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証、および前記プリペイド情報媒体への課金を前記プリペイド情報管理サーバに要求する手段と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記端末に対して前記有料サービスのコンテンツを提供する手段と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記許可ＩＤを生成して前記端末に送信する手段と、
前記端末から前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料サービスのコンテンツを提供する手段とを備え、
前記プリペイド情報管理サーバは、前記端末に対して前記認証用演算情報を送信する手段と、
前記プリペイド情報媒体のパスワードを用いた所定の認証手順により前記プリペイド情報媒体の認証を行う手段と、
前記プリペイド利用ＩＤを基にデータベースを検索し、当該プリペイド利用ＩＤのプリペイド情報媒体の残金に対する課金処理を行う手段と、
前記コンテンツサーバに対して、認証及び課金の完了通知を送信する手段とを備えることを特徴とする有料サービス提供システム。

【請求項９】　前記プリペイド情報管理サーバは、前記コンテンツサーバに対して、暗号鍵として使用される認証用情報を送信する手段を備え、
前記コンテンツサーバは、前記プリペイド情報管理サーバから送信された認証用情報を共通鍵として有料サービスのコンテンツを暗号化する手段を備え、
前記端末は、前記認証情報を共通鍵として、前記暗号化された有料サービスのコンテンツを復号化する手段とを更に備えることを特徴とする請求項８に記載の有料サービス提供システム。

【請求項１０】　前記認証用情報は、前記プリペイド情報管理サーバから前記端末に対して送信される認証用演算情報、あるいは、前記端末において、前記認証用演算情報とパスワードとを結合した値に対して所定の演算を行った演算結果であることを特徴とする請求項９に記載の有料サービス提供システム。

【請求項１１】　端末に対して有料サービスのコンテンツを提供するコンテンツサーバであって、
前記端末から、取引に必要な所定の情報を保持するプリペイド情報媒体を利用する有料サービス利用の要求に応じて、ネットワークを介して接続されるプリペイド情報管理サーバに対して、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金とを要求する手段と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記端末に対して前記有料サービスのコンテンツを提供する手段と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して前記端末に送信する手段と、
前記端末から前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料サービスのコンテンツを提供する手段とを備えることを特徴とするコンテンツサーバ。

【請求項１２】　前記端末にサービスメニューを送信する手段と、
前記端末のアドレス情報と前記有料サービスの課金情報とを前記プリペイド情報管理サーバに転送する手段と、
前記プリペイド情報管理サーバから送信される認証用情報を共通鍵として有料サービスのコンテンツを暗号化する手段を備えることを特徴とする請求項１１に記載のコンテンツサーバ。

【請求項１３】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおける、前記端末を制御する有料サービス提供用プログラムであって、
取引に必要な所定の情報を保持するプリペイド情報媒体を利用して前記コンテンツサーバにサービスメニューを要求させる手順と、
ユーザが利用したいサービスを選択すると、前記コンテンツサーバに対して有料サービスの利用を要求させる手順と、
前記プリペイド情報管理サーバからの要求に基づき、前記プリペイド情報媒体に格納されたプリペイド利用ＩＤを前記プリペイド情報管理サーバに送信させる手順と、
前記プリペイド情報管理サーバから送信された認証用演算情報を用いて、前記プリペイド情報媒体のパスワードに対して所定の演算を行い、その演算結果を前記プリペイド情報管理サーバに送信させる手順と、
前記コンテンツサーバから、前記有料サービスのコンテ

ンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを受信させる手順と、
前記コンテンツサーバから有料サービスのコンテンツをダウンロードさせる手順と、
前記有料サービスのコンテンツのダウンロードが不成功の場合に、前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求を、前記コンテンツサーバに対して要求させる手順とを、前記端末に実行させることを特徴とする有料サービス提供用プログラム。

【請求項１４】　前記認証用演算情報を共有鍵として用いて、前記コンテンツサーバからダウンロードさせた、暗号化された前記有料サービスのコンテンツを復号化させる手順を備えることを特徴とする請求項１３に記載の有料サービス提供用プログラム。

【請求項１５】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおける、前記コンテンツサーバを制御する有料サービス提供用プログラムであって、
前記端末からの要求に基づき、前記端末に対してサービスメニューを送信させる手順と、
前記端末から、取引に必要な所定の情報を保持するプリペイド情報媒体を利用する有料サービスの利用の要求に応じて、前記プリペイド情報管理サーバに対して、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金を要求させる手順と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記端末に対して前記有料サービスのコンテンツを提供させる手順と、
前記プリペイド情報管理サーバからの認証、および課金の完了通知に基づき、前記有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して前記端末に送信させる手段と、
前記端末から前記許可ＩＤを用いて、再度前記有料サービスのコンテンツのダウンロード要求があった場合に、前記端末に対して、前記一定限度内において前記有料サービスのコンテンツを提供させる手順とを、コンテンツサーバに実行させることを特徴とする有料サービス提供用プログラム。

【請求項１６】　前記プリペイド情報管理サーバから受信した認証用演算情報を共有鍵として、前記有料サービスのコンテンツを暗号化させて、前記有料サービスのコンテンツを前記端末に提供させる手順を備えることを特徴とする請求項１５に記載の有料サービス提供用プログラム。

【請求項１７】　端末と、前記端末に対してコンテンツを提供するコンテンツサーバと、有料サービスの課金処理を行うプリペイド情報管理サーバとがネットワークに接続されている有料サービス提供システムにおける、前記プリペイド情報管理サーバを制御する有料サービス提供用プログラムであって、
前記コンテンツサーバからの、前記プリペイド情報媒体が前記コンテンツの有料サービスを利用する資格を有するか否かの認証と、前記プリペイド情報媒体への課金の要求に基づき、前記プリペイド情報媒体に格納されているプリペイド利用ＩＤの送信を要求させる手順と、
当該プリペイド利用ＩＤを受信した後、認証用演算情報を前記端末に対して送信させる手順と、
前記端末から、前記認証用演算情報を用いて前記プリペイド情報媒体のパスワードに所定の演算を施した演算結果を受信した後、前記認証用演算情報を用いてデータベースに格納されている前記プリペイド情報媒体の前記パスワードに、前記端末が使用した演算と同一の演算を行い、その演算結果を前記端末から送信された演算結果と照合して、前記プリペイド情報媒体の認証を行わせる手順と、
前記プリペイド利用ＩＤを基にデータベースを検索し、当該プリペイド利用ＩＤのプリペイド情報媒体の残金と前記コンテンツサーバからの前記課金要求金額を参照して課金処理を行わせる手順と、
前記認証と前記課金処理が共に成功した場合に、前記端末に対して、有料サービス利用手続の完了情報とプリペイド情報媒体の残高を含む情報を、また、前記コンテンツサーバに対して、認証及び課金の完了通知を送信させる手順と、前記プリペイド情報管理サーバに実行させることを特徴とする有料サービス提供用プログラム。

【請求項１８】　前記コンテンツサーバに対して、前記プリペイド情報の前記認証用演算情報を送信させる手順を備えることを特徴とする請求項１７に記載の有料サービス提供用プログラム。

【請求項１９】　請求項１３ないし請求項１８のいずれか１項に記載の有料サービス提供用プログラムを格納したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、有料サービス提供方法、有料サービス提供システム、コンテンツサーバ、有料サービス提供プログラム、および記録媒体に係わり、特に、プリペイドのＩＣカード等の媒体を用い、インターネットを介して端末に有料コンテンツを安全に且つ確実に提供する際に有効な技術に関する。

【０００２】

【従来の技術】コンテンツサーバからインターネットを介して、端末に有料サービスのコンテンツを提供する場合に、端末において有料コンテンツを受信した後に、課金することが難しいことに鑑み、このような有料コンテンツの料金の徴収方法として、以下に示す二種類の方法

が知られている。

（一）その１つは、一般のクレジットカードを利用する信用取引であり、（二）他の１つはプリペイドによる方法である。しかしながら、一般のクレジットカードを利用する場合、カード会社への会員手続きや、預金残金の管理が必要であり、その上、ネットワーク上をクレジット番号が流れることによる盗聴の危険性があるという問題点があった。これに対して、プリペイドによる方法は、クレジットカードを所有しない人でも利用可能であるという特徴を有し、その一例として、例えば、特開平１１－３１６７２９号公報（「インターネット課金方法及びシステム及びインターネット課金プログラムを記録した記録媒体」）が知られている。

【０００３】以下に、プリペイドによる方法の従来例として、特開平１１－３１６７２９号に開示された発明（以下、先行発明と言う。）について詳細に説明する。先行発明は、クレジットカードを所有しない人でも利用可能で、かつ、望ましくない発注を確実に排除可能なインターネット課金方法及びシステム及びインターネット課金プログラムを格納した記録媒体を提供することを目的としたものであり、図８により、先行発明の動作の概要を説明する。先ず、プリペイドカード（ＩＣカード、フロッピー（登録商標）ディスク、磁気カード等）に設定されたコンテンツサーバのアドレス情報（例えば、ＨＴＴＰにおけるＵＲＬ）に基づいて、端末からコンテンツサーバに対し有料サービス利用要求が発行される（ステップ１０１）。次に、コンテンツサーバは、プリペイドカードの認証及び課金処理を行うことをカード管理サーバに要求する（ステップ１０２）。次に、カード管理サーバは、端末との間でカードの認証を行い（ステップ１０３）、認証・課金処理結果をコンテンツサーバに返却する（ステップ１０４）。次に、コンテンツサーバは、認証及び課金処理が成功した場合、有料サービスを端末に提供する（ステップ１０５）。

【０００４】図９は、先行発明の接続構成の概要を示すブロック図である。端末１００は、インターネット４００を介してコンテンツサーバ２００との間でコネクション（サービス開始要求用コネクション）１１を設定し、当該コネクション１１を利用して有料サービスの利用を要求する。コンテンツサーバ２００は、端末１００からの有料サービス利用要求を受け付けると、カード管理サーバ３００との間にコネクション（課金・認証要求用コネクション）１２を設定し、当該コネクション１２を利用して、端末１００のＩＰアドレス（Internet Protocol Addres）を送信することにより、プリペイドカードの認証要求及び課金処理要求を行う。カード管理サーバ３００は、コンテンツサーバ２００からの認証要求を受けると、端末１００との間にコネクション（認証処理用コネクション）１３を設定し、端末１００に対してプリペイドカードのパスワードの演算を要求する。端末１００は、コネクション１３を利用して、カード管理サーバ３００にパスワードの演算結果を送信する。

【０００５】カード管理サーバ３００は、各カードのカード識別子（以下、カードＩＤという）、パスワード、サービス利用ポイント残度数を記憶したカード管理データベース（以下、カード管理ＤＢという。）５００を保持している。カード管理サーバ３００は、カードＩＤからパスワードを検索し、端末１００と同一の演算を行ない、送られてきた演算結果と一致すれば、認証成立とする。カード管理サーバ３００は、認証処理、および課金処理終了後、認証結果及び課金処理結果をコンテンツサーバ２００に通知する。認証処理及び課金処理が成立した場合に、コンテンツサーバ２００は、端末１００に対して有料サービスのコンテンツの提供を開始する。認証処理、または、課金処理が成立しなかった場合に、コンテンツサーバ２００は、端末１００に対してコネクション１１を利用してカードが使用不可能であることを通知する。

【０００６】図１０は、先行発明の概略システム構成を示すブロック図である。プリペイドカードに設定されたコンテンツサーバアドレス情報に基づいてコンテンツサーバ２００にアクセスし、コンテンツサーバ２００の提供する有料サービスの利用を要求する端末１００と、当該端末１００からの要求を受けて端末１００に対して有料サービスを提供するコンテンツサーバ２００と、コンテンツサーバ２００からの要求を受けてプリペイドカードの認証と、プリペイドカードに対する課金を行うカード管理サーバ３００とで構成される。

【０００７】端末１００は、サービス要求部１０１、およびカード管理部１０２を有する。サービス要求部１０１は、プリペイドカードに設定されたコンテンツサーバアドレス情報（ＵＲＬ等）に基づいて、コンテンツサーバ２００との間に自動的にコネクションを確立し、有料サービスの利用を要求する。サービス要求部１０１は、例えば、ＷＷＷブラウザで構成できる。カード管理部１０２は、プリペイドカードの形態に応じた読み取り装置を介してプリペイドカード１０３と接続され、カード管理サーバ３００からの要求に基づいて、プリペイドカードに格納されたカードＩＤを送信する機能と、カード管理サーバ３００からの要求に基づいてプリペイドカードに格納された機密情報（パスワード等）を読み出し、一方向性関数等による演算処理を行なった後にカード管理サーバ３００に送信する機能と、カード管理サーバ３００からの要求に基づいて、プリペイドカードにプリペイドカード残高、利用日時を書き込む機能とを有する。

【０００８】コンテンツサーバ２００は、認証要求部２０１、課金処理要求部２０２、サービス提供部２０３、およびカード管理部２０４を有する。認証要求部２０１は、端末１００から有料サービスの利用要求があった場合に、カード管理サーバ３００に対してプリペイドカー

ドが正しいものかどうかの認証要求を行う機能を有し、課金処理要求部２０２は、カード管理サーバ３００に対してプリペイドカードに対する課金を要求する機能を有する。サービス提供部２０３は、認証処理、および課金処理が共に成功した場合に、端末１００に対して有料サービスを提供する機能を有し、カード管理部２０４は、認証要求部２０１、および課金処理要求部２０２に対してプリペイドカードの認証、課金を要求する機能を有する。

【０００９】カード管理サーバ３００は、認証部３０１、課金処理部３０２、およびカード管理ＤＢ５００を有し、認証部３０１は、コンテンツサーバ２００からの認証要求があった場合に、端末１００に対してプリペイドカードの認証を行う機能を有する。課金処理部３０２は、有料サービスの利用度合いに応じた課金処理をプリペイドカードに対して実施する機能と、端末１００に対してプリペイドカードの残高、利用日時を通知する機能を有する。カード管理ＤＢ５００は、各カードのカードＩＤ、パスワード、サービス利用ポイント残度数を記録している。

【００１０】先行発明におけるシステム動作シーケンスを図１１に示す。ここでは、有料サービスとしてＶｉｄｅｏの配信、認証方法としてＲＦＣ１３３４で規定されているChallenge Response方式（W.Simpson,"PPPChallenge Handshake Authentication Protocol(CHAP)",Aug 1996）を使用する例を用いて説明する。初めに、端末１００は、プリペイドカードに設定されたコンテンツサーバアドレス情報（例えば、ＵＲＬ）を用いて、当該アドレスを有するコンテンツサーバ２００との間にコネクションを設定し、サービスメニューを要求する（ステップ２０１）。次に、コネクションが設定されると、コンテンツサーバ２００からＶｉｄｅｏのリストなどのサービスメニューが送信される（ステップ２０２）。次に、ユーザが利用したいサービスを選択すると、コンテンツサーバ２００に対して、選択したサービスを利用するために必要なサービス利用ポイント数が設定されたサービス利用要求メッセージが送信される（ステップ２０３）。

【００１１】次に、コンテンツサーバ２００は、カード管理サーバ３００との間にコネクションを設定し、当該コネクションを利用して、端末１００のＩＰアドレスを設定した認証要求メッセージを送信することにより、カード管理サーバ３００に対してプリペイドカードが正しいプリペイドカードか否かの認証要求を行う（ステップ２０４）。また、同時に、カード管理サーバ３００に対して利用サービスのサービス度数を設定した課金処理要求メッセージを送信することにより、課金処理を要求する。なお、認証要求メッセージと課金処理要求メッセージは同一のメッセージであっても、別々のメッセージであっても実施可能である。次に、カード管理サーバ３００は、受信した認証要求メッセージ中の端末１００のＩＰアドレスに基づいて、端末１００との間にコネクションを設定し、当該コネクションを利用して、端末１００にカードＩＤを要求する（ステップ２０５）。

【００１２】次に、端末１００は、プリペイドカードに格納されたカードＩＤをカード管理サーバ３００に送信する（ステップ２０６）。次に、カード管理サーバ３００は、端末１００との間に設定したコネクションを利用して、認証用の乱数（チャレンジ）を端末１００に対して送信する（ステップ２０７）。この乱数は、端末１００の認証を行うたびに異なる値が使用される。次に、乱数を受信した端末１００は、乱数とパスワードとを結合した値に対してＭＤ５ｎ（RivestR and S.Dusse,"The MD5 Message-Digest Algorithm",April1992）などの一方向性関数で演算を行い、その結果（レスポンス）を設定した応答メッセージをカード管理サーバ３００に送信する（ステップ２０８）。

【００１３】次に、カード管理サーバ３００は、カード管理ＤＢ５００に保持しているプリペイドカードのパスワードと端末１００に送信した乱数とを統合した値に対して端末が使用したのと同じ一方向性関数により演算を行い、その結果を端末１００からの応答と照合する。両者が一致すれば、認証成立とし（ステップ２０９）、両者が一致しなければ認証不成立とする。このように、カード管理サーバ３００は、カードの認証に毎回異なる乱数を使用するので、第三者がチャレンジとレスポンスを盗聴したとしても、次の認証時にその値を使って端末１００のユーザになりすますことはできない。また、レスポンスに一方向性関数による演算値を使用するので、第３者がレスポンスを知り得たとしても、元のパスワードを推定することはできない。

【００１４】次に、カード管理サーバ３００は、カードＩＤを基にカード管理ＤＢ５００を検索し、該当するカードのサービス利用ポイントの残度数が、課金処理要求メッセージに設定されたサービスポイントより大きければ、該当するカードのサービス利用ポイントを課金処理要求メッセージに設定されたサービスポイント数だけ減算する（ステップ２１０）。該当するカードのサービス利用ポイントの残度数が、課金処理要求メッセージに設定されたサービスポイントより小さければ、課金処理不可能とし、処理を終了する。なお、認証・課金処理不可能の場合、処理を終了する。次に、カード管理サーバ３００は、端末１００に対してプリペイドカードの残高、利用日時を通知し（ステップ２１１）、また、コンテンツサーバ２００に対して、認証・課金処理結果を通知する（ステップ２１２）。最後に、コンテンツサーバ２００は、端末１００に対して有料サービスを提供する（ステップ２１３）。

【００１５】図１２は、先行発明の端末１００の処理手順を示すフローチャートである。以下、図１２を用いて、端末１００の処理手順について説明する。先ず、プ

リペイドカードに記録されているアドレス情報に基づいて、コンテンツサーバ２００との間にコネクションを設定し、サービスメニューをコンテンツサーバ２００に対して要求する（ステップ３０１）。次に、設定したコネクションを利用して、サービスの所要ポイント数が設定されたサービス利用要求メッセージをコンテンツサーバ２００に送信する（ステップ３０２）。次に、カード管理サーバ３００からの要求に基づいて、プリペイドカードに格納されているカードＩＤをカード管理サーバ３００に送信する（ステップ３０３）。

【００１６】次に、カード管理サーバ３００からの要求に基づいて、プリペイドカードに格納されている機密情報（パスワード等）を読み出し、一方向性関数等による演算処理を行なった後に、カード管理サーバ３００に送信する（ステップ３０４）。認証、および課金が成功した場合、カード管理サーバ３００から残高が通知され（ステップ３０５）、有料サービスのコンテンツの提供を受けることができる（ステップ３０６）。なお、カード管理サーバ３００から通知される残高の値は、端末１００に表示されると共に、プリペイドカードに残高、利用日時を書き込むことができる。認証、または課金が失敗した場合、有料サービスは提供されない（ステップ３０７）。

【００１７】図１３は、先行発明のコンテンツサーバの処理手順を示すフローチャートである。以下、図１３を用いて、コンテンツサーバの処理手順について説明する。先ず、端末１００からサービスメニューの要求があると、サービスメニュー一覧を端末１００に送信し（ステップ４０１）、端末１００から有料サービス利用要求を受信する（ステップ４０２）。次に、認証・課金要求メッセージのカードＩＤ部にカードＩＤ、端末アドレス部に端末アドレス、サービスポイント部に利用するサービスの所要ポイント数をそれぞれ設定し、当該メッセージをカード管理サーバ３００に送信することにより、カード管理サーバ３００に対してカードの認証及びカードに対する課金を要求する（ステップ４０３）。なお、この例では、カード管理サーバ３００が端末１００にカードＩＤを要求するため、カードＩＤは設定しない。

【００１８】但し、その他の例として、端末１００からコンテンツサーバ２００に有料サービス要求を送信する時にカードＩＤを送信する方法、およびコンテンツサーバ２００からの要求に基いて、端末１００がコンテンツサーバ２００にカードＩＤを送信する方法がある。これらの場合は、カードＩＤが設定される。次に、認証及び課金が成立したか否かを判断し（ステップ４０４）、ステップ４０４でＹＥＳの場合には、端末１００に対して有料サービスのコンテンツの提供を開始する（ステップ４０５）。ステップ４０４でＮＯの場合には、端末１００に対して、認証又は課金処理が成立しなかったことを通知する（ステップ４０６）。

【００１９】図１４は、先行発明のカード管理サーバの処理手順を示すフローチャートである。以下、図１４を用いて、カード管理サーバ３００の処理手順について説明する。先ず、コンテンツサーバ２００からの認証・課金要求メッセージを受信する（ステップ５０１）。当該メッセージにカードＩＤが設定されていない場合には、受信した認証・課金要求メッセージ中の端末１００のＩＰアドレスに基づいて、端末１００との間にコネクションを設定し、当該コネクションを利用して、端末１００にカードＩＤを要求する（ステップ５０１－１）。また、当該メッセージにカードＩＤが設定されている場合には、認証用の乱数（チャレンジ）を端末１００に対して送信する（ステップ５０２）。この乱数は、端末１００の認証を行うたびに異なる値が使用される。なお、この場合に、端末１００との間にコネクションが設定されていないときには、受信した認証・課金要求メッセージ中の端末１００のＩＰアドレスに基づいて端末１００との間にコネクションを設定し、当該コネクションを利用して、認証用の乱数（チャレンジ）を端末１００に対して送信する。

【００２０】次に、端末１００からの応答（レスポンス）を受信し、カード管理ＤＢ５００で保持しているプリペイドカードのパスワードと端末１００に送信した乱数とを統合した値に対して、端末が使用したのと同じ一方向性関数により演算を行い、その結果を端末１００からの応答と照合することにより認証処理を行なう（ステップ５０３）。次に、両者が一致したか否かを判断し（ステップ５０４）、ステップ５０４でＮＯの場合には、認証不成立として処理を終了する。また、ステップ５０４でＹＥＳの場合には、課金可能か否かを判断する（ステップ５０５）。即ち、該当するカードのサービス利用ポイントの残度数と、課金処理要求メッセージに設定されたサービスポイントとを比較する。

【００２１】ステップ５０５で、該当するカードのサービス利用ポイントの残度数が、課金処理要求メッセージに設定されたサービスポイントより大きければ、該当するカードのサービス利用ポイント残度数を課金処理要求メッセージに設定されたサービスポイントだけ減算する（ステップ５０６）。次に、端末１００に対して、プリペイドカードの残高、利用日時を通知し（ステップ５０７）、認証・課金処理結果をコンテンツサーバ２００に通知する（ステップ５０８）。ステップ５０５で、該当するカードのサービス利用ポイントの残度数が、課金処理要求メッセージに設定されたサービスポイントより小さければ、課金不可能であるので、処理を終了する。

【００２２】なお、前述の説明において、認証方法としては、前述した以外の方法を使用しても良いことはいうまでもない。また、提供する有料サービスとしては、Ｖｉｄｅｏの配信以外に、プログラムなどのデータのダウンロード、オンラインショッピングなどがある。また、

パスワードをカードに内蔵させずに、ユーザ自身が入力するようにしてもよい。また、前述の手順において、認証が成功してから、コンテンツサーバがカード管理サーバに課金処理を要求する構成とすることも可能であり、更に、プリペイドの形式としては、金額やポイント、その他任意の形態が可能である。

【００２３】

【発明が解決しようとする課題】前述したように、従来例では、プリペイドカードの認証処理及び課金処理が正しく完了した場合のみ、端末からの有料サービス要求を受け付けるので、望ましくない発注を確実に排除することができる。更に、先行発明では、コンテンツサーバ２００が、カード管理サーバ３００に端末１００のアドレス情報を送信し、カード管理サーバ３００から直接端末１００にアクセスして、端末上のプリペイドカードを認証できる。したがって、プリペイドカードのパスワード等の機密情報が不正なコンテンツサーバに漏洩することを確実に防ぐことができる。しかしながら、コンテンツサーバ３００からの有料情報配信前に課金の引き落としが行われるため、端末１００とコンテンツサーバ２００のコネクションを解除した後に、コンテンツが正常にダウンロードできなかったことが分かると、端末１００はコンテンツサーバにアクセスする手段が残されていないという問題点があった。

【００２４】この問題は、モバイル環境での使用においても容易に生じ得る問題である。このような問題を解決する発明として、特開２０００－２７０３０９号「情報配信に対する課金および精算システム並びにそのサーバ」がある。特開２０００－２７０３０９号では、サーバは端末にダウンロードすべきコンテンツ料金をプリペイド料金から引き落とした後、有料情報を端末にダウンロードし、そして、端末がダウンロードにより受信した情報量を調べ、受信量をサーバに送る。サーバは送信量と受信量を比較し、両者が不一致のときは受信が上手く行かなかったと判断し、その相当分を返金する方式である。この方式によれば、全体を受信しないと意味がないコンテンツに対しても一定比率の返金しかできないという問題があり、複雑な制御をしても無意味になることがあり得る。

【００２５】本発明は、前記従来技術の問題点を解決するためになされたものであり、本発明の目的は、有料サービス提供方法および有料サービス提供システムにおいて、クレジットカードを所有しない人でも利用可能で、望ましくない発注を確実に排除可能なだけでなく、有料コンテンツの正常なダウンロードも可能にし、不正なダウンロードも防止することが可能となる技術を提供することにある。また、本発明の他の目的は、前述の有料サービス提供システムに使用されるコンテンツサーバを提供することにある。また、本発明の他の目的は、前述の有料サービス提供方法を、コンピュータに実行させる制御プログラムを提供することにある。また、本発明の他の目的は、前述のプログラムが記録された記録媒体を提供することにある。本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【００２６】

【課題を解決するための手段】本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記の通りである。即ち、本発明は、有料サービス提供方法であって、コンテンツサーバが、有料サービスのコンテンツのダウンロードを一定限度内の範囲で有効とする許可ＩＤを生成して端末に送信し、端末が、有料サービスのコンテンツを正常に受信できなかった場合に、前述の許可ＩＤを使用して、有料サービスのコンテンツが正常に受信できるまで繰り返してコンテンツサーバにアクセス可能としたことを特徴とする。これにより、有料サービスのコンテンツの配信前に、予め課金しておいても、ユーザが確実に有料サービスのコンテンツを入手することが可能となる。

【００２７】また、本発明は、有料サービス提供方法であって、カード認証を行うプリペイド情報管理サーバが、プリペイド情報媒体の認証用に端末に送信した認証演算情報（あるいは、認証演算結果）をコンテンツサーバに提供し、コンテンツサーバが、当該認証演算情報（あるいは、認証演算結果）を共通鍵として用いて、有料サービスのコンテンツを暗号化して、端末に提供し、端末は、認証段階で使用した認証演算情報（あるいは、認証演算結果）を共通鍵として用いて、提供された暗号化されたコンテンツを復号化することを特徴とする。これにより、ダウンロードしたコンテンツが、他に漏れても内容が分からないことや、ダウンロード許可ＩＤをユーザ以外の人が不正使用しても共通鍵がない限り復号できないことから、ユーザだけに有料のコンテンツが確実に届いたかどうかを判断することができ、ユーザ、並びにコンテンツサーバの両者に効果がある。

【００２８】また、本発明は、有料サービス提供方法であって、端末に接続するＩＣカード、フロッピーディスク、磁気カード等のプリペイド情報媒体内にパスワードを保持せず、ユーザが端末を操作して外部から入力することを特徴とする。これにより、このパスワードを使用できるユーザのみが、ダウンロードする権利を得ることになり、プリペイド情報媒体の安全性を向上させ、第三者の不正なダウンロードを防止することができる。また、本発明は、前述の有料サービス提供方法を実現するための有料サービス提供システム、およびコンテンツサーバである。また、本発明は、前述の有料サービス提供方法を実現するための、端末、コンテンツサーバ、並びに、プリペイド情報管理サーバの各々の制御を行う有料サービス提供用プログラムである。また、本発明は、前述のプログラムを格納するコンピュータ読み取り可能な

記録媒体である。

【００２９】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。なお、実施の形態を説明するための全図において、同一機能を有するものは同一符号を付け、その繰り返しの説明は省略する。本明細書において、ユーザが、コンテンツサーバにサービス利用を要求する際に使用するプリペイド情報媒体を、以下、プリペイドカードと称するが、本発明において、プリペイド情報媒体は、カードの形態に限定されるものではない。また、プリペイド情報管理サーバを、以下、カード管理サーバと称するが、カード管理に限定されるものではない。プリペイドカードは、例えば、カード管理会社が発行・管理するものであり、ユーザは、有料サービスを利用するためにプリペイドカードを購入する。プリペイドカードには、コンテンツサーバアドレス情報、カードＩＤ、カードパスワード等が設定されており、購入金額に応じて利用可能なサービスの残高（金額又はポイント等）は、プリペイド情報管理サーバすなわちカード管理サーバが管理している。

【００３０】本発明は、先行発明（特開平１１－３１６７２９号に記載の発明）を、ユーザが確実に有料コンテンツを入手できるとともに、その不正防止を行えるように改良したものである。したがって、本発明の実施の形態の有料サービス提供システムは、図１０に示す先行発明と、そのシステム構成は同じであるので、本実施の形態の有料サービス提供システムのシステム構成の説明は省略する。図１は、本発明の実施の形態の有料サービス提供システムの動作の概要を説明するためのシーケンスチャートである。図１において、ステップ１０４までは、図８に示す先行発明のシーケンスチャートと同じであり、ステップ１０５以降が、先行発明と異なっている。コンテンツサーバは、認証及び課金処理が成功した場合、有料サービス提供の許可を端末に与える（ステップ１０５）。端末は、一定期間等の限度内で複数回ダウンロードすることが許可され、コンテンツサーバは有料情報を提供する（ステップ１０６，１０７）。

【００３１】図２は、本発明の実施の形態の接続構成の概要を示すブロック図であり、同図において、コネクション１４が、図９に示す先行発明の接続構成と異なっている。このコネクション１４は、端末１００が、ダウンロードアクセスをコンテンツサーバ２００に要求する場合のコネクションであり、他のコネクション（１１～１３）が解放された後に張られる場合がある。本実施の形態の有料サービス提供システムの構成は、端末１００のサービス要求部１０１が、コンテンツサーバ２００から有料サービスのコンテンツのダウンロードＩＤを受け、そのダウンロードＩＤを用いて確実に受信できるまで一定の制限内でダウンロード要求を行うことができる点が先行発明と相違する。また、コンテンツを暗号化する場合は、コンテンツサーバ２００のサービス提供部２０３と、端末１００のサービス要求部１０１に機能が付与されるが、他は先行発明と同様である。なお、この図２では、端末１００、コンテンツサーバ２００、並びに、カード管理サーバ３００を接続するネットワークとして、インターネットを使用する場合について説明したが、端末１００、コンテンツサーバ２００、並びに、カード管理サーバ３００を接続するネットワークとして、一般の電話回線などの公衆通信回線網も使用可能である。

【００３２】次に、本実施の形態の有料サービス提供システムの一連の動作の一例について、図３を用いて具体的に説明する。図３は、本実施の形態の有料サービス提供システムにおける一連の動作の一例を説明するためのシーケンスチャートである。図３において、ステップ２１２までは、図１１に示す先行発明のシーケンスチャートと同じであるので、説明を省略して相違点のみ説明する。コンテンツサーバ２００は、カード管理サーバ３００からサービス提供許可（即ち、認証・課金処理結果）が通知されると（ステップ２１２）、端末１００に対して有料サービスのコンテンツのダウンロードアクセスを一定の制限下で許可するＩＤを提供し（ステップ２１４）、次に、端末１００に対して有料サービスを提供する（ステップ２１３）。この許可ＩＤが有効な「制限下」とは、発注した同一コンテンツを一定のアクセス期間以内（例えば、２４時間以内）、若しくは、一定のアクセス回数以内（例えば、１０回以内）、または、これらの組み合わせ（例えば、１０回以内、または、２４時間以内の何れか制限に達した方）をいう。

【００３３】なお、図３では図示していないが、この許可ＩＤは確実に端末１００に到達している必要がある。そのような方法としては、①複数の同一ＩＤを繰り返し送り、多数決をとることで確認する方法、②コンテンツサーバ２００から端末１００に送信したＩＤを再度コンテンツサーバ２００に送り返して照合する方法等が知られている。この場合、①の方法では受信側で、②の方法では送信側で正常性を判断できる。この許可ＩＤが正常受信できた後、有料サービスを提供する。ステップ２１３で、有料サービスが正常に受信できなかった場合、ユーザは、端末１００からダウンロード許可ＩＤをコンテンツサーバ２００に送信し（ステップ２１５）、コンテンツサーバ２００から有料サービスのコンテンツのダウンロードを行う（ステップ２１６）。この場合、許可ＩＤが一定の制限内であって有効であることを確認し、条件によってはアクセスカウント数を増加する制御を行う。更に、発注段階の端末のＵＲＬと同一かどうかの照合を行えば、端末確認が可能になる。

【００３４】次に、本実施の形態の有料サービス提供システムの一連の動作の他の例について、図４を用いて具体的に説明する。図４は、本実施の形態の有料サービス提供システムにおける一連の動作の他の例を説明するた

めのシーケンスチャートである。図４において、ステップ２１１までは、図１１に示す先行発明のシーケンスチャートと同じであるので、説明を省略して相違点のみ説明する。カード管理サーバ３００は、端末１００の認証及び課金が終了するとコンテンツサーバ２００にサービス提供許可（即ち、認証・課金処理結果）を送信する（ステップ２１７）。図４に示す例は、それに暗号鍵を追加する点で、図３に示す例と相異する。暗号鍵としては、カード管理サーバ３００から端末１００にステップ２０７で送信した認証用情報である乱数やそれを基に端末１００が演算した認証情報が利用できる。これらは端末１００も既に保有している情報であることから、復号化するときに共通鍵として利用できる。

【００３５】次に、コンテンツサーバ２００は、カード管理サーバ３００から送られた暗号鍵によりコンテンツを暗号化する（ステップ２１８）。次に、コンテンツサーバ２００は、端末１００に対して有料サービスのコンテンツのダウンロードアクセスを一定の制限下で許可するＩＤを提供し（ステップ２１４）、端末１００に対して有料サービスを提供する（ステップ２１３）。端末１００は、コンテンツサーバ２００からダウンロードした、暗号化された有料サービスのコンテンツ情報に対し、端末１００にある共通鍵で復号化する（ステップ２１９）。なお、ステップ２１５、２１６のアクセス方法は、図３に示す例と同じである。

【００３６】図５は、本実施の形態の端末１００の処理手順を示すフローチャートである。以下、図５を用いて、本実施の形態の端末１００の処理手順について説明する。なお、図５において、ステップ３０７までは、図１２に示す先行発明の端末１００の処理手順と同じであるので、説明を省略して相違点のみ説明する。端末１００は、ステップ３０５でカード管理サーバ３００から残高が通知された後に、ダウンロード許可ＩＤを正常受信できたことを確認するステップ（３０８，３０９）。正常受信の判断は、前述のステップ２１４で述べたように端末１００でも、コンテンツサーバ２００側でも実効可能である。次に、コンテンツサーバ２００から有料サービスのコンテンツのダウンロードを行う（ステップ３１０）。このコンテンツを受信するステップ３１０では、例えば、モバイル環境等の場合、正常に受信できない場合もあり得る。

【００３７】次に、コンテンツが暗号化されているときは、復号化を行う（ステップ３１１）。本実施の形態では、端末認証に用いた一過性の乱数情報を共通鍵に使用しているので、更なる暗号鍵の配信が不要であり安全性が高いという特徴がある。本実施の形態において、端末１００へのアクセスは、サービス開始前の場合と、有料サービスのコンテンツのダウンロードが不成功に終わった場合とがあるが、ステップ３０１で、端末１００へのアクセスがいずれの場合のアクセスかを判断する。ステップ３０１で判断結果が、サービス開始前の場合は、ステップ３０２～３１１の処理を実行する。ステップ３０１での判断結果が、有料サービスのコンテンツのダウンロードをリトライする場合には、先ず、許可ＩＤにより、コンテンツサーバ２００に対してアクセスを行う（ステップ３１３）。コンテンツサーバ２００が、許可ＩＤが有効か否かを、端末１００のアドレス情報等の情報と併せて確認し、コンテンツサーバ２００が再度のダウンロードを許可する場合には、ステップ３１０、ステップ３１１の処理（有料サービスのコンテンツのダウンロード処理）に移行し、許可できないときはその旨が表示される（ステップ３１４）。

【００３８】図６は、本実施の形態のコンテンツサーバ２００の処理手順を示すフローチャートである。以下、図６を用いて、本実施の形態のコンテンツサーバ２００の処理手順について説明する。なお、図６において、ステップ４０６までは、図１３に示す先行発明のコンテンツサーバ２００の処理手順と同じであるので、説明を省略して相違点のみ説明する。端末認証がカード管理サーバ３００で成功した場合で、さらに、コンテンツを暗号化する場合、コンテンツサーバ２００には、カード管理サーバから、共通鍵として使用される情報（例えば、端末認証に使用した情報）が送られてくる。コンテンツサーバ２００は、カード管理サーバ３００から送られてくる情報を受信し、この情報を共通鍵にして、コンテンツを暗号化する（ステップ４０７）。なお、共通鍵として使用される情報は、認証用に使用した情報であって、端末１００と共有できるもの（例えば、カード管理サーバ３００から端末１００に送られた認証用演算情報、あるいは、それを用いてカード利用ＩＤと演算した結果など）であれば、何れも使用可能である。

【００３９】次に、ダウンロード許可ＩＤを生成し（ステップ４０８）、このダウンロード許可ＩＤを端末１００に対して送信し（ステップ４０９）、端末１００においてダウンロード許可ＩＤが正常に受信できたかを判断する（ステップ４１０）。ステップ４１０で、端末１００において、ダウンロード許可ＩＤが正常に受信できなかったと判断された場合には、ステップ４０９、ステップ４１０を繰り返す。ステップ４１０で、端末１００において、ダウンロード許可ＩＤが正常に受信できたと判断された場合には、コンテンツサーバ２００から端末１００への有料サービスのコンテンツのダウンロードを行う（ステップ４１１）。なお、ステップ４０８における、コンテンツサーバ２００での許可ＩＤの生成は、安全性の観点からは、ランダムな生成が望ましいが、運用上の独自のルールで作成することもできる。

【００４０】本実施の形態において、コンテンツサーバ２００に対する端末１００からのアクセスは、サービスの初期段階の場合と、有料サービスのコンテンツのダウンロードのリトライの場合とがあるが、ステップ４０１

で、コンテンツサーバ２００に対する端末１００へのアクセスがいずれの場合かを判断する。端末１００からのアクセスが、サービスの初期段階の場合は、ステップ４０１～ステップ４１１の処理を実行する。端末１００からのアクセスが、有料サービスのコンテンツのダウンロードのリトライの場合には、許可ＩＤが限度内かを判断し（ステップ４１３）、ステップ４１３で、許可ＩＤが限度外と判断された場合には、許可ＩＤが無効であることを端末１００に通知する（ステップ４１６）。ステップ４１３で、許可ＩＤが限度内と判断された場合には、その許可ＩＤに付随する端末１００のアドレス情報等の情報を読み出し、要求のあった端末１００と一致するかを照合し（ステップ４１４）、正当な使用かどうかを判断する（ステップ４１５）。ステップ４１５で、正当な使用と認証された場合には、ステップ４１１に進み、端末１００への有料サービスのコンテンツのダウンロードを行う。ステップ４１５で、正当な使用でないと認証された場合には、認証不成功を端末１００に通知する（ステップ４１７）。

【００４１】図７は、本実施の形態のカード管理サーバ３００の処理手順を示すフローチャートである。以下、図７を用いて、本実施の形態のカード管理サーバ３００の処理手順について説明する。なお、図７において、ステップ５０７までは、図１４に示す先行発明のカード管理サーバ３００の処理手順と同じであるので、説明を省略して相違点のみ説明する。本実施の形態では、コンテンツサーバ２００に送る情報は、ＩＣカード等の認証結果とプリペイドの残高が有料サービスを提供できる範囲にあることを確認する情報であるが、必要により、暗号鍵を送信する（ステップ５０９）。これにより、コンテンツサーバ２００は、より安全な情報提供が可能になる。なお、暗号鍵としては、端末１００と共有できる情報であって、前述のステップ４０７で説明したものがある。また、改めて再度配送すれば、その他の共通鍵や公開鍵も使用できる。

【００４２】以上説明したように、本実施の形態によれば、クレジットカードを所有しない人でも有料情報（有料サービスのコンテンツ）を入手可能であり、課金後に情報提供が上手く行かなかった場合でもダウンロードを繰り返し実行できる権利を利用者に与えることにより、ユーザ環境等の不具合があっても確実に情報を入手することが可能になる。また、情報提供者の立場ではダウンロードのリトライを許すことにより契約外のユーザにも利用される危険があるが、端末１００のアドレスと許可ＩＤを併用し、更に期間とアクセス回数等の組み合わせの範囲内で有効にしていることにより、不正使用を最小限に抑えられる効果がある。

【００４３】なお、前述の説明において、認証方法としては、前述した以外の認証方法を使用しても良いことはいうまでもない。また、提供する有料サービスとしては、Ｖｉｄｅｏの配信以外に、プログラムなどのデータのダウンロード、オンラインショッピングなどがあり、プリペイドカードの実現形態としては、ＩＣカードやフロッピーディスク、磁気カード等がある。また、パスワードをカードに内蔵させずに、ユーザ自身が入力するようにしてもよい。また、前述の手順において、認証が成功してから、コンテンツサーバ２００が、カード管理サーバ３００に課金処理を要求する構成とすることも可能である。さらに、プリペイドの形式としては、金額やポイント、その他任意の形態が可能である。

【００４４】残高情報は、プリペイドカードに記録しても良いが、本実施の形態では、カード管理サーバ３００で管理する残高情報に基づいて処理されることから、プリペイドカードへの書き込みは行わずに、カード管理サーバ３００上で一元的に管理しておくと残高情報の不一致が生ずる危険を回避できる。また、このようにすることで、プリペイドカードの盗難等の災害時でも、第３者が、残高を容易に知ることができなくなり、特にパスワードを、カード内に記録しておかないときはその効果は顕著であるという利点がある。なお、本発明は、前述の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能であることはいうまでもない。

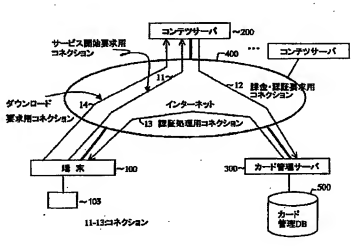
【００４５】また、前述の説明においては、主にプリペイドカードへの適用について説明したが、本発明は、航空会社のマイレッジカードのみならず、百貨店、ホテル、ソフト販売（ＣＤ、ビデオ、ゲームソフト等）、ビデオやＣＤレンタル、スーパー、家電販売、ガソリンスタンド等の幅広い業界で使用されているポイントカードを利用した決済システムに適用可能である。本発明では、ダウンロードが認められたＩＤを使用する点で会員サービスにおけるユーザＩＤと類似している。多くの場合、会員サービスにおいては一旦会員になってしまうと、その期間を意識することは殆どなく、個々のアクセス回数等を記録しておく等の処置は不要である。

【００４６】しかしながら、本発明では、有料サービスのコンテンツのダウンロードを一定限度内で有効にした許可ＩＤを使用していることから、ユーザは、その限度を個々の商品毎にアクセス回数、使用期間等を管理する手段を要する点で異なっており、ユーザが購入し代金を支払ったものを確実に入手できる権利の保証を与えているとみなすことができる。このような管理を行うことは、販売業者にとっても許可ＩＤの不正使用のリスクを最小限にすることを保証している。特に、図４に示す例では、端末認証した情報で、コンテンツを暗号化しているので、許可ＩＤを不正に使用しても容易に情報を入手できないという特徴がある。以上、本発明者によってなされた発明を、前記実施の形態に基づき具体的に説明したが、本発明は、前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００４７】
【発明の効果】本顧において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記の通りである。
（１）本発明によれば、クレジットカードを所有しない人でも、有料サービスのコンテンツを入手可能であるとともに、ユーザ環境等の不具合で、課金後に情報提供が上手く行かなかった場合でも、確実に情報を入手することが可能になる。
（２）本発明によれば、端末のアドレスと許可ＩＤを併用し、更に期間とアクセス回数等の組み合わせの範囲内で有効とすることにより、不正使用を最小限に抑えることが可能となる。
【図面の簡単な説明】
【図１】本発明の実施の形態の有料サービス提供システムの動作の概要を示すシーケンスチャートである。
【図２】本発明の実施の形態の有料サービス提供システムの接続構成の概要を示すブロック図である。
【図３】本実施の形態の有料サービス提供システムにおける一連の動作の一例を説明するためのシーケンスチャートである。
【図４】本実施の形態の有料サービス提供システムにおける一連の動作の他の例を説明するためのシーケンスチャートである。
【図５】本発明の実施の形態の端末の処理手順を示すフローチャートである。
【図６】本発明の実施の形態のコンテンツサーバの処理手順を示すフローチャートである。
＊【図７】本発明の実施の形態のカード管理サーバの処理手順を示すフローチャートである。
【図８】先行発明の有料サービス提供システムの動作の概要を示すシーケンスチャートである。
【図９】先行発明の有料サービス提供システムの接続構成の概要を示すブロック図である。
【図１０】先行発明の有料サービス提供システムのシステム構成を示すブロック図である。
【図１１】先行発明の有料サービス提供システムにおける一連の動作を説明するためのシーケンスチャートである。
【図１２】先行発明の端末の処理手順を示すフローチャートである。
【図１３】先行発明のコンテンツサーバの処理手順を示すフローチャートである。
【図１４】先行発明のカード管理サーバの処理手順を示すフローチャートである。
【符号の説明】
１１…サービス開始要求用及びダウンロード用コネクション、１２…課金・認証要求用コネクション、１３…認証処理用コネクション、１４…ダウンロード要求用コネクション、１００…端末、１０１…サービス要求部、１０２…カード管理部、１０３…プリペイドカード、２００…コンテンツサーバ、２０１…認証要求部、２０２…課金処理要求部、２０３…サービス提供部、２０４…カード管理部、３００…カード管理サーバ、３０１…認証部、３０２…課金処理部、４００…インターネット、５００…カード管理ＤＢ。

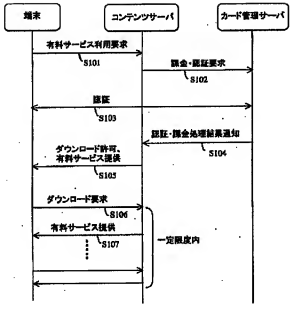
【図２】

図２



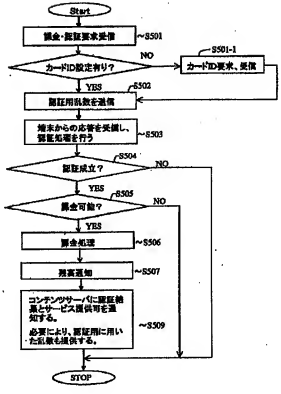
【図１】

図１



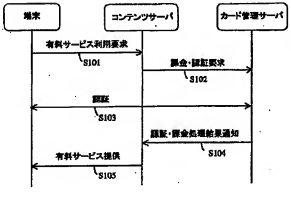
【図７】

図７



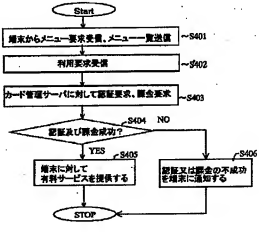
【図８】

図８



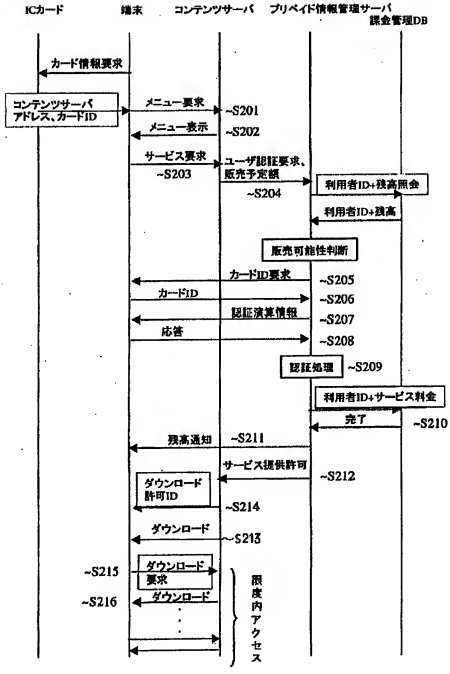
【図１３】

図１３



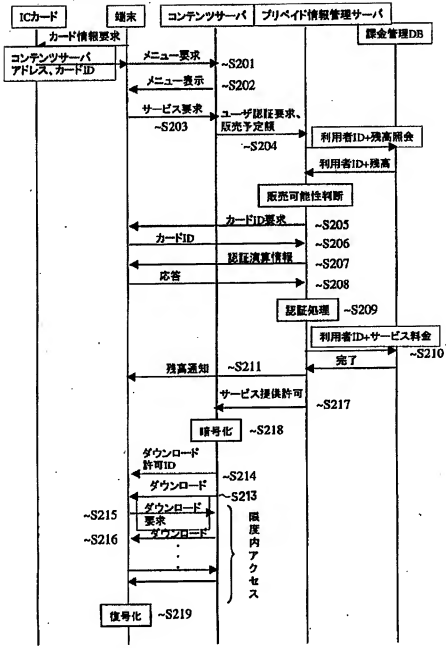
【図３】

図３


ICカード
端末
コンテンツサーバ
プリペイド情報管理サーバ
課金管理DB
カード情報要求
コンテンツサーバ
アドレス、カードID
メニュー要求
~S201
メニュー表示
~S202
サービス要求
~S203
ユーザ認証要求、
販売予定額
~S204
利用者ID+残高照会
利用者ID+残高
販売可能性判断
カードID要求
~S205
カードID
~S206
認証演算情報
~S207
応答
~S208
認証処理
~S209
利用者ID+サービス料金
完了
~S210
残高通知
~S211
サービス提供許可
~S212
ダウンロード
許可ID
~S214
ダウンロード
~S213
~S215
ダウンロード
要求
~S216
ダウンロード
限度内アクセス

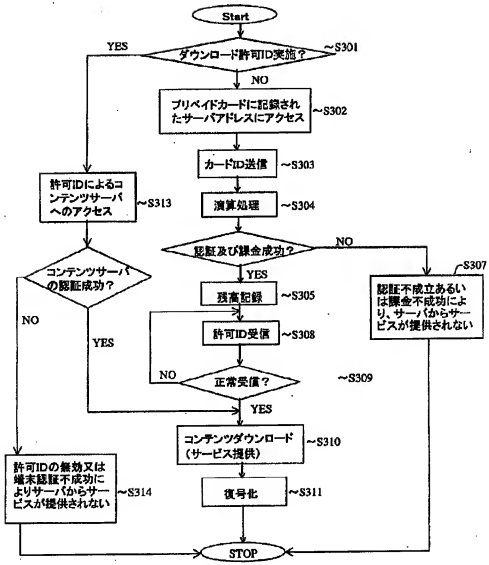
【図４】

図４


ICカード
端末
コンテンツサーバ
プリペイド情報管理サーバ
課金管理DB
カード情報要求
コンテンツサーバ
アドレス、カードID
メニュー要求
~S201
メニュー表示
~S202
サービス要求
~S203
ユーザ認証要求、
販売予定額
~S204
利用者ID+残高照会
利用者ID+残高
販売可能性判断
カードID要求
~S205
カードID
~S206
認証演算情報
~S207
応答
~S208
認証処理
~S209
利用者ID+サービス料金
~S210
完了
残高通知
~S211
サービス提供許可
~S217
暗号化
~S218
ダウンロード
許可ID
~S214
ダウンロード
~S213
~S215
ダウンロード
要求
~S216
ダウンロード
限度内アクセス
復号化
~S219

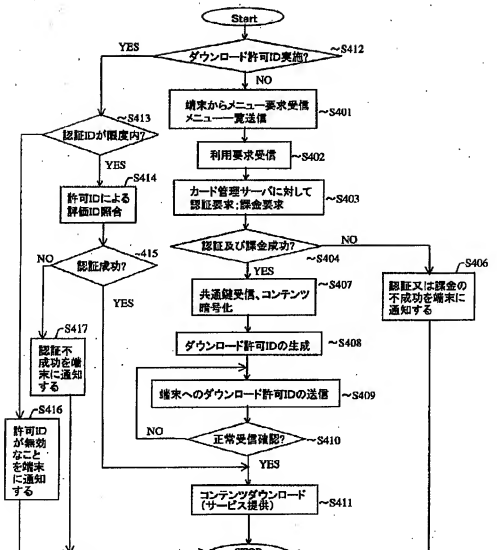
【図５】

図５


Start
ダウンロード許可ID実施？
S301
YES
NO
プリペイドカードに記録されたサーバアドレスにアクセス
S302
カードID送信
S303
演算処理
S304
認証及び課金成功？
S307
NO
YES
残高記録
S305
許可ID受信
S308
正常受信？
S309
NO
YES
コンテンツダウンロード（サービス提供）
S310
復号化
S311
許可IDによるコンテンツサーバへのアクセス
S313
コンテンツサーバの認証成功？
NO
YES
認証不成立あるいは課金不成功により、サーバからサービスが提供されない
許可IDの無効又は端末認証不成功によりサーバからサービスが提供されない
S314
STOP

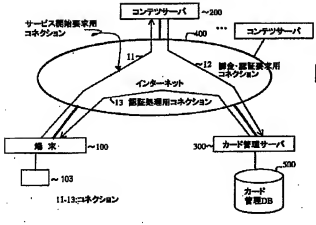
【図６】

図６


Start
ダウンロード許可ID要求?
S412
YES
NO
端末からメニュー要求受信
メニュー一覧送信
S401
認証IDが限度内?
S413
YES
利用要求受信
S402
S414
許可IDによる
課価ID照合
カード管理サーバに対して
認証要求;課金要求
S403
認証及び課金成功?
NO
S404
YES
S406
認証又は課金の
不成功を端末に
通知する
S415
NO
認証成功?
YES
S407
共通鍵受信、コンテンツ
暗号化
S417
認証不
成功を端
末に通知
する
ダウンロード許可IDの生成
S408
端末へのダウンロード許可IDの送信
S409
S416
許可ID
が無効
なこと
を端末
に通知
する
NO
正常受信確認?
S410
YES
コンテンツダウンロード
(サービス提供)
S411
STOP

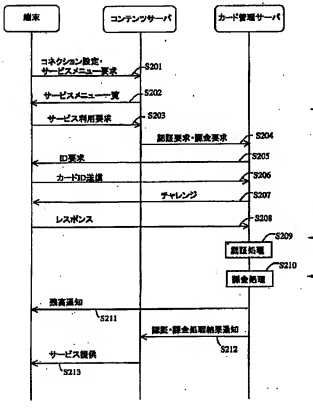
【図９】

図９



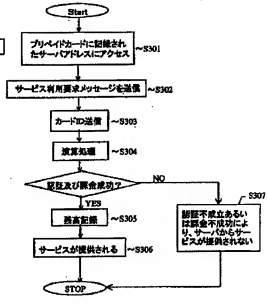
【図１１】

図１１



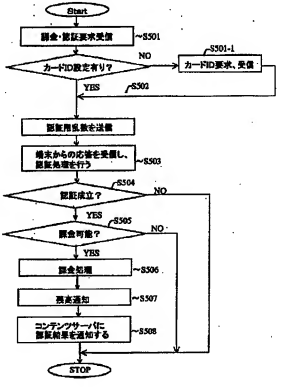
【図１２】

図１２



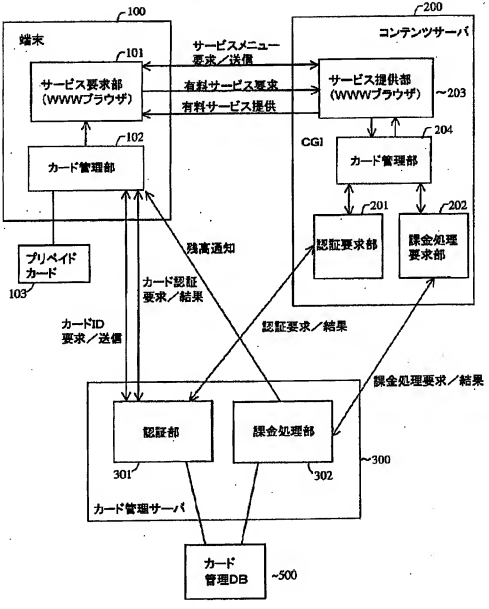
【図１４】

図１４



【図１０】

図１０



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
G06F 17/60	512	G06F 17/60		512
15/00	330		15/00	330Z
H04L 9/08		H04L 9/00		601E
9/32				673B

675A
675D